[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

ManageWise® 2.6
Network Management Guide

ManageWise®

MANAGEMENT SOFTWARE

Novell.

Contents

3 Tailoring Maps and Object Data

IV Handling Alarms

6 Understanding Alarms

7 Network and Device Alarms

V Maintaining Your Network and Its Devices

8 Managing Servers

9 Managing Workstations

10 Managing Routers

11 Managing Hubs

12 Managing SNMP Devices

13 Analyzing Your Network

14 Testing Connectivity

15 Managing Network Addresses

VI ManageWise Management Strategies

16 Using ManageWise to Maintain Network Performance

A Using Remote Console

Glossary

Index

Introducing ManageWise

Part I provides an overview of ManageWise® software. Specifically, this part describes

◆ The purpose of each ManageWise component and agent

◆ ManageWise features, such as maps and alarms

◆ The ManageWise database and the types of information it contains

◆ The devices you can manage, such as servers, workstations, and routers, and the information you can get about them

1 *ManageWise Overview*

ManageWise® software provides SNMP-compliant network monitoring and management capabilities for networks that comprise products from multiple vendors. Together with the agents, ManageWise manages and monitors the performance of NetWare® servers, Ethernet, token ring and FDDI network segments, workstations, and routers, as well as hubs that comply with the Hub Management Interface™ (HMI™) specification. In addition, ManageWise automatically discovers your network and the objects attached to it.

ManageWise forms a distributed system, which means that although you can manage the network from a central location (the ManageWise Console), certain system components (management agents) are deployed throughout the network.

ManageWise includes the following:

◆ The ManageWise software, with these major components:

- ◆ ManageWise Console software

- ◆ NetExplorer™ system

◆ ManageWise agents, available separately:

- ◆ NetWare Management Agent™ software

- ◆ NetWare LANalyzer® Agent™ software

Note For version compatibility information about NetExplorer Server software, ManageWise agents, and NetWare, refer to the MWREADME.WRI file.

You can deploy some or all the ManageWise components in the way that best meets your management needs.

ManageWise Components

ManageWise includes the ManageWise Console and the NetExplorer system components.

ManageWise Console

The ManageWise Console software is a Windows application that provides an integrated interface for managing your NetWare networks. The ManageWise Console provides a graphical user interface, a database of all network information, an alarm management system, and NetExplorer Manager.

NetExplorer

NetExplorer, the network discovery system, is installed on a ManageWise Server and communicates with routers, NetWare servers, and NetWare LANalyzer Agent software to discover your network segments, routers, servers, HMI hubs, and workstations. (A ManageWise Server running the NetExplorer network discovery software is referred to as the *NetExplorer Server.*) NetExplorer organizes the information it discovers and sends it to the ManageWise Console. This forms most of the data in the ManageWise database.

When you first install ManageWise, it has no information about your network. You use NetExplorer to gather the information that lets you monitor and manage your network.

ManageWise Agents

ManageWise agents are deployed at strategic locations in the network and perform five main functions:

◆ They record and maintain statistics that reflect the state of the system and make them available to the ManageWise Console for historical analysis

◆ They capture packets and make them available to the ManageWise Console for later analysis

◆ They log information for historical analysis using the ManageWise Console

◆ They watch for problem conditions and report them to the ManageWise Console

◆ They carry out commands issued by the ManageWise Console

Agents are typically assigned very specific tasks, such as keeping watch over a specific NetWare server (NetWare Management Agent) or overseeing a network segment (NetWare LANalyzer Agent).

NetWare Management Agent

NetWare Management Agent software provides real-time server performance data and information about server alarms to the ManageWise Console. It should be deployed on each server you want to manage from the ManageWise Console. Server management is explained in Chapter 8, "Managing Servers."

NetWare LANalyzer Agent

NetWare LANalyzer Agent software enables a NetWare server to monitor all traffic on Ethernet, token ring or FDDI network segments to which the server is attached. A single NetWare server running NetWare LANalyzer Agent can monitor several network segments simultaneously. Segment management is explained in Chapter 13, "Analyzing Your Network."

NetWare Hub Services Agent

NetWare Hub Services agent enables both local and remote management of server-based hubs that comply with the HMI specification. This agent also lets you monitor hub performance, monitor each node attached to a hub, and enable or disable network access to nodes connected to the hub. Hub management is explained in Chapter 11, "Managing Hubs."

Using ManageWise to Manage a Network

After ManageWise and its agents are installed, you can use ManageWise to help you manage your network. The following sections describe how to do so.

ManageWise Maps

ManageWise provides two different types of maps of your network. You can use these maps to see your network and the connections between your network objects:

◆ Logical maps, which ManageWise creates automatically based on data it discovers

◆ Custom maps, which you create

In addition, ManageWise lets you create objects that you can either add to maps or use to create an entire topology from scratch. You can add objects such as workstations, NetWare servers, hubs, routers, bridges, segments, and third-party objects.

Logical Maps

As network data arrives from NetExplorer and is written into the ManageWise database, ManageWise begins to build maps of your network. Your entire network, its segments, connections, and nodes appear in ManageWise logical maps.

ManageWise automatically provides two types of logical maps:

◆ **Internetwork map**—Shows segments and routers and the logical connections between them in your internetwork

◆ **Segment map**—Shows the servers, workstations, routers, and other nodes for each segment on your internetwork map
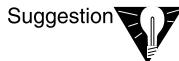
Suggestion — You can use maps as a navigation tool to other parts of the system. For example, if you see an alarm icon above a NetWare server on a segment map, you can select the server and open an Alarm Report to see alarms affecting that server.

Custom Maps

In addition to the logical maps, ManageWise provides an editor that you can use to create your own views, or *custom maps*, of your network, floor plans, buildings, or any collection of objects you are interested in.

Suggestion   You can connect your custom maps with each other and with ManageWise logical maps of your network. Then you can copy objects to your custom map by dragging icons from ManageWise maps to your custom maps. When you do so, the alarms on internetwork and segment maps are also propagated onto the custom maps.

For more detailed information about ManageWise maps, refer to Part II, "Understanding Maps."

Alarm System

The ManageWise alarm system alerts you to errors and other conditions on the network. Alarms come from several sources:

◆ From any node that supports SNMP and sends SNMP traps to the ManageWise Console

◆ From NetExplorer as it discovers the network

◆ From programs running on the ManageWise Console

◆ From an error detected during a connectivity test

Alarm Severity, State, and Disposition

All alarms are assigned a default severity, state, and disposition, but you can override the default values. Alarm severity values indicate the seriousness of the alarm; state values represent the operational status of the affected object; disposition settings indicate actions that the system takes when an alarm of that type arrives.

Visual Presentation

You know that an alarm has occurred when you see a bell-shaped graphic above an object icon in a map. If an alarm is reported for an object, it is shown on all maps that include the object. For example, an alarm appearing on a node on an internetwork map also appears on a custom map having the same node.

The color of the bell and its placement within the rectangle above the object icon represent the alarm severity. The color of object icons changes dynamically according to the operational status of the object, as indicated by alarms received by the ManageWise Console. A nonoperating object is shown with a grayed-out icon.

Alarm Tables

You can look at the alarms in more detail using the Alarm Report or the Alarm Monitor windows.

◆ **Alarm Report window**—Displays alarms that have been logged in the database. It can display all logged alarms or only alarms that apply to a certain object. The Alarm Report also lets you delete, acknowledge, or add comments to alarms and view NetWare Expert™ help.

◆ **Alarm Monitor window**—Starts when you start the ManageWise Console. It displays a table of the last 400 alarms received.

The types of alarms that ManageWise can receive and display are determined by the Management Information Bases (MIBs) that ManageWise has compiled. Many MIBs are shipped with ManageWise; some MIBs are precompiled for the installation and others can be compiled separately, depending on your network needs. The ManageWise Tools menu provides a utility to compile MIBs, as explained in Chapter 12, "Managing SNMP Devices."

Refer to Chapter 6, "Understanding Alarms," for more information about the ManageWise alarm system.

ManageWise Database

The ManageWise database contains all the data about the network. The database covers several interrelated areas of information:

- ◆ **Network topology**—Includes the networks, segments, nodes on segments, adapter boards connected to segments, addresses applicable to nodes, and services such as routing, file services, print services, and so forth.

- ◆ **Custom map data**—This data is not automatically discovered and entered into the database. However, you can enter this as optional information.

- ◆ **Configuration**—Each object in the database might also contain special attributes that identify details about that object. For example, special attributes include the operating system, the number and size of disk drives, and the amount of RAM in a node. You can enter this information in the database.

- ◆ **Alarm system configuration**—Configuration of your alarm dispositions can be saved in the database.

- ◆ **Logged alarms**—Selected alarms can be saved in the database.

- ◆ **Class information**—The database also includes information about itself and the types of objects it knows about. Third-party developers can add to the types of objects that ManageWise knows about. When they do this, they add to the class information. Objects in a new class act just like ManageWise objects.

ManageWise provides tools for maintaining the database. For more information about maintaining the database, refer to Part II, "Understanding Maps."

NetWare Server Management

ManageWise can manage any NetWare server on which you have installed NetWare Management Agent software (a managed server), which responds to SNMP management data requests from the ManageWise Console and also transmits alarms from the server to the ManageWise Console.

For each managed server, you can obtain the following real-time information:

◆ Configuration data

  ◆ Interface adapters

  ◆ Adapters

  ◆ Bound protocols

  ◆ Open files

  ◆ Installed software

◆ Loaded NLM™ (NetWare Loadable Module™) files

◆ Disk and volume usage

◆ Memory usage

◆ CPU utilization

◆ Trend data

◆ User and connection information

◆ Print queues and print status

◆ Alarms from thresholds you set

In addition, ManageWise provides two more features useful for managing servers:

◆ A Windows version of RCONSOLE

◆ Integration with NetWare Administrator

For more information about managing servers and monitoring their dynamic performance data, refer to Chapter 8, "Managing Servers." For information about RCONSOLE, refer to Appendix A, "Using Remote Console."

Workstation Management

ManageWise can manage any workstation that has the workstation agent software loaded.

ManageWise provides information about workstations using these graphical displays:

◆ **NetWare Client™ window**—Displays information about workstations, including a traffic graph, the NetWare shell and DOS versions, MAC address, lists of attached servers and corresponding login names, drive mappings, and print queues.

◆ **Diagnostic Details window**—Displays Internetwork Packet Exchange™ (IPX™) counters, Sequenced Packet Exchange™ (SPX™) counters, and LAN driver counters. These counters track events relevant to IPX, SPX, and the LAN driver, such as the number of packets sent by each.

For more information about monitoring workstation data and collecting diagnostic information, refer to Chapter 9, "Managing Workstations."

Router Management

ManageWise provides the following windows you can use to monitor routers and their interfaces.

◆ **Routers Summary table**—Summarizes all routers in your internetwork. This table also provides access to further details, such as system addresses and interface monitoring.

◆ **Router Interfaces Statistics table**—Shows performance statistics for the interfaces of selected routers. You can also display line graphs of all the statistics for an interface.

◆ **IPX Routers window**—Summarizes all IPX routers in your database. This table also provides access to further details, such as configuration, statistics, and NetWare Link Services Protocol™ (NLSP™) topology.

For more information about monitoring routers and router interfaces, refer to Chapter 10, "Managing Routers."

Network Addresses and Connectivity

ManageWise provides tools you can use to manage network addresses and test connectivity.

◆ **Managing addresses**—The ManageWise Console provides three network tables you can use as planning tools for assigning IPX, IP, and NetWare/IP™ addresses:

◆ **IPX Networks table**—Lists all IPX network numbers discovered in your internetwork.

◆ **IP Networks table**—Lists all IP networks and individual subnet masks.

◆ **NetWare/IP table**—Lists all NetWare IP nodes belonging to a selected domain.

For more information about network addresses, refer to Chapter 15, "Managing Network Addresses."

◆ **Testing connectivity**—The Connectivity Test facility lets you monitor critical objects in your internetwork and manage potential connectivity problems before they affect the network.

For more information about connectivity, refer to Chapter 14, "Testing Connectivity."

Network Segment Management

ManageWise can manage any Ethernet, token ring, or FDDI network that is monitored by NetWare LANalyzer Agent. This agent continually monitors network segments by

◆ Collecting statistics on traffic patterns

◆ Watching for alarm conditions

◆ Capturing packets according to criteria you set

Agents can monitor and capture all packets on the network, whether they are generated by servers running NetWare or by other nodes.

You can manage a segment by selecting it from a map or table and choosing a menu item or button that brings up a window or dialog box. ManageWise automatically determines which agent monitors the selected segment and communicates with it as necessary to obtain the desired data.

For more information about managing segments, refer to Chapter 13, "Analyzing Your Network."

Hub Management

ManageWise can manage any HMI-compliant hub installed in a NetWare server that is running the NetWare Hub Services agent. This agent allows both local and remote management of these hubs on Ethernet, or token ring networks.

The ManageWise Console lets you perform these hub management tasks:

◆ Configure hubs and the individual ports on a hub

◆ Enable or disable ports

◆ Name individual ports and refer to the ports by name

◆ Remotely test hubs to check their operating status

The ManageWise Console provides information about all HMI hubs on the network through these graphical displays:

◆ **Hub Backpanel window**—Displays an overview of the condition of all ports on a selected hub server.

◆ **Hub Port map**—Displays details about your hubs, including the condition of each port and the object connected to it.

◆ **Statistics graphs**—Display information including port utilization, byte and frame rates, error rates, and the numbers of errors.

For more information about managing HMI-compliant server hubs, refer to Chapter 11, "Managing Hubs."

SNMP Object Management

ManageWise lets you manage any SNMP-manageable objects on your network. In particular, you can

◆ Receive alarms (SNMP traps)

◆ Use the SNMP MIB Browser tool to display and set values

The SNMP MIB Browser tool lets you talk to any SNMP-manageable object over either TCP/IP or IPX to get information to or change a value of the object.

For more information about SNMP and the ManageWise MIB Browser, refer to Chapter 12, "Managing SNMP Devices."

Online Help

ManageWise provides two types of online help:

◆ **NetWare Expert**—When the ManageWise Console receives an alarm about an event or condition on the network, it displays the alarm notification in a window, where you can find expert help about that type of alarm. The NetWare Expert help describes the alarm, shows the default severity, tells you the significance of the alarm, and suggests actions to take.

◆ **General and context-sensitive help**—Help is available at every point of ManageWise. You can search through the entire system using the Help menu, and you can find context-sensitive help by pressing the F1 key or clicking the Help button in most ManageWise windows.

Third-Party Software You Can Use with ManageWise

Many third parties have written software that runs with ManageWise. Novell has compiled a list of many of the products into a booklet called *ManageWise Solutions Guide*. Call your Novell technical representative or 1-800-NETWARE to request a copy of this booklet.

part

II   *Understanding Maps*

Part II describes the types of maps ManageWise® software creates, gives suggestions on how to use them, and explains how to create custom maps and add and change information on your maps.

This part also discusses the ManageWise database. The ManageWise database is a set of files in which ManageWise stores data about the discovered network topology, the physical location of nodes, node configuration information, and information about alarms. Using the database, ManageWise builds various views of this information, including maps. Entering new information in the database can change the maps, and changing the maps can affect the database.

chapter **2** *Using Maps*

ManageWise® software includes three types of maps:

◆ **Internetwork maps** display the segments and routers on your internetwork and the logical connections between them. Figure 2-1 shows an internetwork map.

◆ **Segment maps**—one for each segment on the internetwork map— displays servers, workstations, routers, and other nodes.

◆ **Custom maps** let you create a physical view of your network. You can, for example, represent the location of networks, segments, and nodes relative to your geographic locations. Alternatively, you can create a map that shows only the servers and routers you monitor daily. Custom maps also let you specify the connection between logical networks (represented by the internetwork and segment maps) and physical networks.

Each map has an action bar across the top, with buttons that provide access to common map functions.

ManageWise maps can also alert you to alarm conditions on the network. To do this, you must set the alarm disposition to save alarms in the database. Upon recognizing a critical, major, or minor alarm on a segment or node, ManageWise displays a bell-shaped alarm icon above the object. For information about alarms, refer to "Changing Alarm Dispositions" on page 137.

Figure 2-1
Sample Internetwork Map
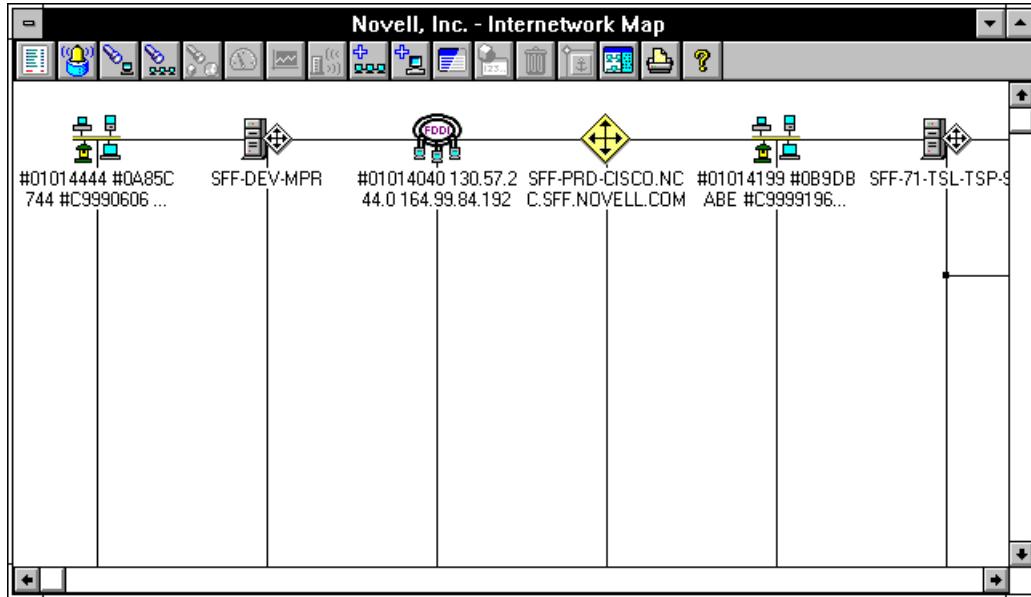
Use internetwork and segment maps to learn about problems and locate their sources and to get information about segments, routers, servers, and workstations. Use custom maps to connect the logical views of the network and its nodes with the physical view of your network, floor plans, buildings, campus, city, and so forth, so you can determine the location of the node or segment that is causing problems.

You can use any map to get information about alarms affecting workstations and other objects. For example, if you want to identify what event caused an alarm, represented by a bell icon appearing next to a specific workstation icon, you can select the workstation icon and open an Alarm Report by clicking the Alarms button or selecting *Fault > Alarm Report.* (Refer to Chapter 6, "Understanding Alarms.")

Displaying a New Portion of a Map

Unless you are looking at a small network or segment, a window shows only part of the map. You can change the portion of the map that is displayed by using one of the following approaches:

◆ Change to view a different section of a map using the Navigator (refer to "Displaying a Specific Map Area").

◆ Scroll a map using scroll bars and keyboard commands (refer to "Moving through the Map" on page 23).

◆ Double-click an object connected to another object drawn earlier and higher on the internetwork map (refer to "Double-Clicking a Connection Reference Object" on page 23).

◆ Display a particular node or instance of a type of node on a segment map by selecting *View > Find* (refer to "Finding Objects on Maps" on page 24) or the action bar buttons.

Displaying a Specific Map Area

To display a different area of the internetwork map or a segment map, use the Navigator. The Navigator is useful for seeing which objects have alarms when your map is larger than what your screen shows. As shown in Figure 2-2, the Navigator displays a small-scale view of the map and shows a great deal more map area than the primary map display.

Figure 2-2
Navigator View
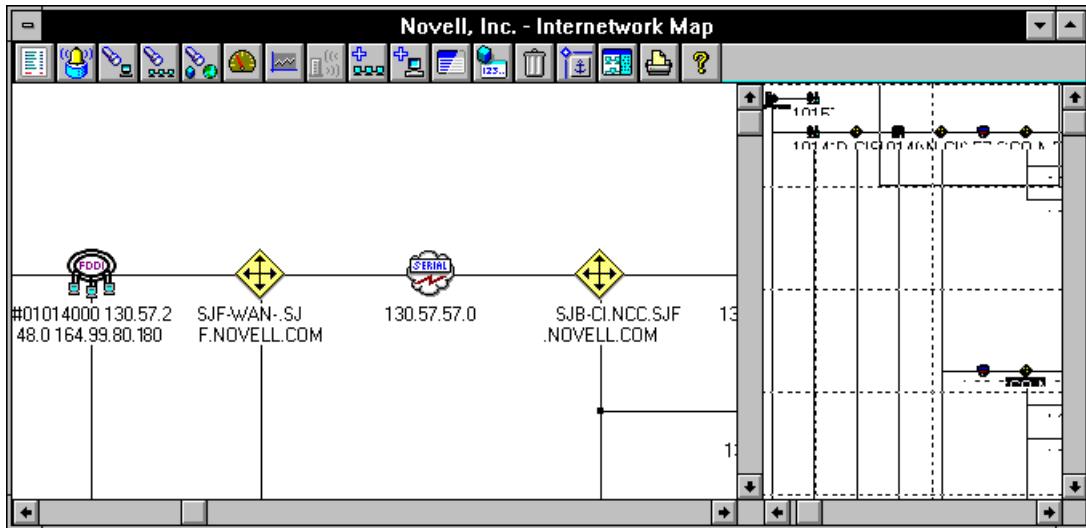
A grid overlies the Navigator view. Each grid square contains a section of the map. One section of the grid shows most of the currently displayed area of the map and has a heavier outline than the others.

To display another area of the map using the Navigator to move the outline to the new area, follow these steps:

Procedure

1. Turn on Navigator by clicking the Navigator button.

The map window splits into two panes. The left pane shows the left side of the original map display. The right pane contains the Navigator.

2. In the Navigator pane, locate the area of the map that you want to display.

If necessary, use the pane scroll bars.

3. **Click the center of the area on the Navigator view that you want to display.**

The Navigator outlines the new area, and the left pane displays the selected section of the map. When you are satisfied with the new display, you can turn off Navigator by clicking the Navigator button again.

Moving through the Map

You can move through maps with a mouse or the following keyboard equivalents:

- ◆ Up-arrow scrolls up 5 percent of the screen

- ◆ Down-arrow scrolls down 5 percent of the screen

- ◆ Left-arrow scrolls left 5 percent of the screen

- ◆ Right-arrow scrolls right 5 percent of the screen

- ◆ PageUp scrolls up one screen height

- ◆ PageDown scrolls down one screen height

- ◆ Home scrolls to the upper-left corner of the map

- ◆ End scrolls to the lower-right corner of the map

Double-Clicking a Connection Reference Object

A connection reference is a connection between one object and another object that was drawn earlier and higher on the internetwork map. The connection reference is shown on the internetwork map as a dotted line. Double-clicking the connection reference changes the view on the internetwork map from the connection reference to the object. Refer to "Internetwork Map Display Format" on page 31 for more information about connection references.

Finding Objects on Maps

You can find all objects that match a search criteria, one at a time, by selecting *View > Find*. To find an object elsewhere on a map, select *View > Find Next*. For more information, refer to "Finding a Node" on this page and "Finding a Segment" on page 28.

After you have selected an object, you can also locate it in other maps. Refer to "Locating an Object in Other Maps" on page 30 for more information.

ManageWise cannot find objects that are filtered from a segment map. To restore a filtered object, select *View > Filter By*. For more information, refer to "Displaying Selected Objects on a Segment Map" on page 39.

You can search for either a node or a segment.

Finding a Node

To find a node on a map, follow these steps:

Procedure
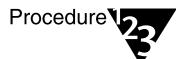
1. **Select *View > Find > Node*, or click the Find Node button on the action bar.**

   ManageWise displays the Find Node dialog box (see Figure 2-3).

Note

By default, the fields in the Find Node dialog box are set to values used the previous time the Find Node command was used.

Figure 2-3
Find Node Dialog
Box
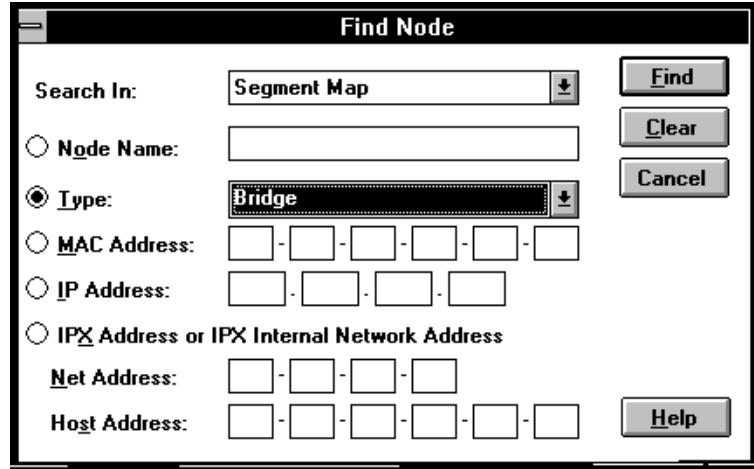
2. **Select the type of map to search.**

   You can select the Active Map (the map that is currently selected), Custom Map, Segment Map, Internetwork Map, or All Maps.

3. **Select the Node Name, Type, or address option button that defines the search key you want to use.**

   Only the parameter that you select is used in the search. Options that you do not select are grayed out. Although a type is shown in the Type list box, it is used only if you select the Type option button.

4. **Enter the name or address for the node you want to find.**

   The search is not case-sensitive. Use the following guidelines to enter the name or address:

   ◆ In Node Name, use any characters.

   ◆ In Type (an object containing a particular service or a particular type of object, like a PC), select from the list box.

   ◆ In MAC Address, use only hexadecimal digits (0–9, A–F).

   ◆ In IP Address, use decimal numbers between 0 and 255.

   ◆ In IPX Address, use only hexadecimal digits (0–9, A–F). The IPX™ address consists of a net address and a host address.

Note ▼ The net address identifies either the segment to which the node is connected or the internal network number of a node. The host address is the node's MAC address or node number.

For any name or address, use either of the following wildcard characters:

◆ "?" matches any single alphanumeric character. Use ? only at the start of the string. For example, if you are searching for MKTG_SERVER1, you would use ????_SERVER1. If you enter any character before the ?, ManageWise displays an error message.

◆ "*" matches zero or more characters starting from the * to the end of the string. Use * only at the end of the string. For example, if you are searching for MKTG_SERVER1, you would use MKTG_*******. The Find command ignores any characters entered after the *.

For any address, each box in the Find Node dialog box must have only characters or only wildcards. For example, the IP address.

| ??? | . | 130 | . | 57 | . | 54 |

is valid, whereas the IP address

| ?00 | . | 130 | . | 57 | . | 54 |

is not.

The following is another example of a valid IP address. This example finds all objects with IP addresses beginning with 123.

| 123 | . | * | . | | . | |

5. Click Find.

If you selected Active Map as the search limit, ManageWise searches only the active window. If you selected All Maps as the search limit, ManageWise begins the search in the active window if there is one, then searches any other open windows and minimized windows, and then searches all other maps of that type. If you limited the search to one type of map, ManageWise searches open and minimized maps of that type first and then continues searching all other maps of that type.

When ManageWise finds the node, it opens the map, displays the node, flashes a box around the icon, and selects it.

If the node is in multiple maps or more than one object satisfies the search criteria, select *View > Find Next* to find other matches. Select *View > Find Next*, or press Ctrl+N, to find all objects matching the search criteria. If you only want to find other instances of the same node, use the Locate action bar button (refer to "Locating an Object in Other Maps" on page 30 for more information).

Finding a Segment

To find a segment on a map, follow these steps:

Procedure
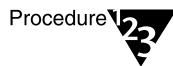
1. Select *View > Find > Segment*, or click the Find Segment button on the action bar.

ManageWise displays the Find Segment dialog box (see Figure 2-4).

Note

By default, the fields in the Find Segment dialog box are set to values used the previous time the Find Segment command was used.

**Figure 2-4
Find Segment
Dialog Box**
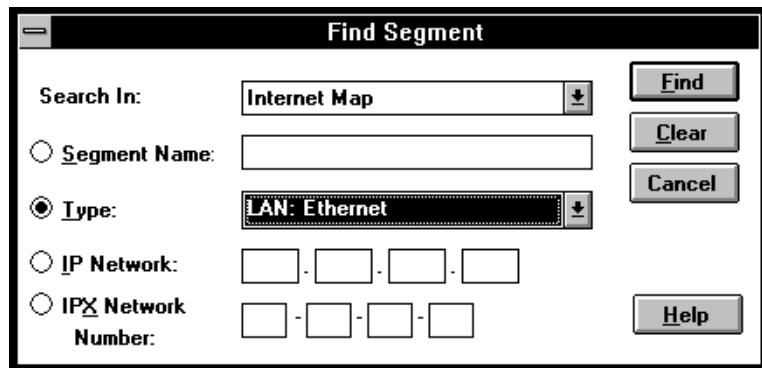
2. Select the maps to search.

You can select the Active Map (the map that is currently selected), Custom Map, Internetwork Map, or All Maps.

3. Select the Name, Type, or address button that defines the search key you want to use.

Only the parameter that you select is used in the find. Options that you do not select are grayed out. Although a type is shown in the Type category list box, it is used only if you select the Type option button.

4. In the appropriate field, enter the name or address for the object you want to find.

The search is not case-sensitive. Use the following guidelines to enter the object name or address:

◆ For a segment name, use any characters.

If the segment name is the same as the segment number, a pound sign (#) precedes the segment name on the internetwork map. For example, a segment with the number C9090906 appears with a segment name of #C9090906 on the internetwork map.

◆ For a type, select from the list box.

◆ For an IP address, use decimal numbers between 0 and 255.

◆ For an IPX network number, use only hexadecimal digits (0–9, A–F).

The IPX network number is the same as the IPX external network number, the number that identifies the segment.

For any name or address, use either of the following wildcard characters:

◆ "?" matches any single alphanumeric character. Use ? only at the start of the string. If you enter any character before the ?, ManageWise displays an error message.

◆ "*" matches zero or more characters starting from the * to the end of the string. Use * only at the end of the string. The Find command ignores any characters entered after the *.

For any address, each box in the Find Segment dialog box must have only characters or only wildcards. For example, the IP address

| ??? | . | 130 | . | 57 | . | 54 |

is valid, whereas the IP address

| ?00 | . | 130 | . | 57 | . | 54 |

is not.

5. **Click Find.**

If you selected Active Map as the search limit, ManageWise searches only the active window. If you selected All Maps as the

search limit, ManageWise begins the search in the active window if there is one, then searches any other open windows and minimized windows, and then searches all maps in the network. If you limited the search to one type of map, ManageWise searches open and minimized maps of that type first and then continues searching all other maps of that type.

When ManageWise finds the segment, it opens the map, displays the segment, flashes a box around the icon, and selects it.

If the segment is in multiple maps or more than one segment satisfies the search criteria, select *View > Find Next* to find other matches. Continue to select *View > Find Next* to find segments matching the search criteria. If you want to find only other instances of the same segment, use the Locate action bar button (refer to "Locating an Object in Other Maps").

Locating an Object in Other Maps

To locate an object in other maps, follow these steps:

Procedure

1. Select the object in an open map.

2. Click the Locate button in the map action bar.

ManageWise displays the Locate in Selected Map dialog box.

For example, in Figure 2-5, the Locate box shows that the selected router can also be found in a number of other maps.

Figure 2-5
Locate in Selected
Map Dialog Box
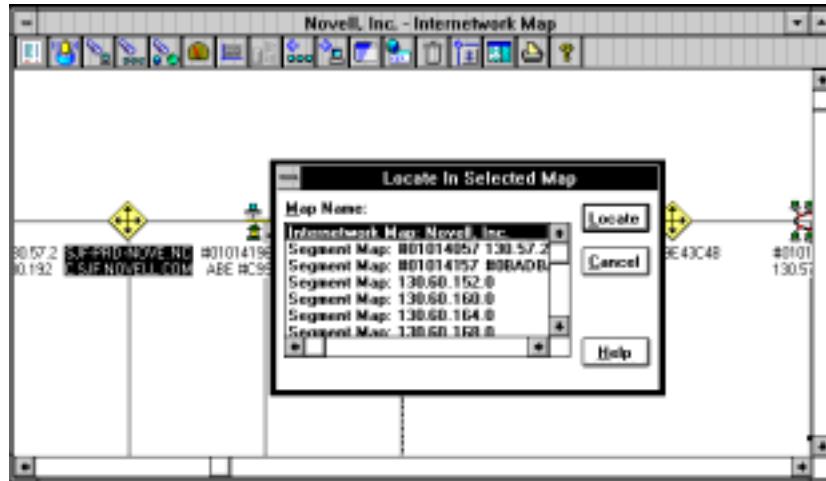
3. **Select the desired map, and then click the Locate button.**

   ManageWise opens the map, displays the object, flashes a box
   around the icon, and selects it.

Viewing Internetwork Maps

The internetwork map provides an overview of the logical organization
of your network. It shows all routers in your database, Ethernet
segments, token ring segments, FDDI segments, and other segment
types.

Note ▼ The NetExplorer™ software does not recognize bridges; therefore, a single
segment icon might represent multiple segments connected by bridges.
Similarly, NetExplorer represents bridging-routers as routers. To correct bridged
segments, select *Edit > Add* (refer to "Troubleshooting Maps" on page 73 for
examples).

To open and display the internetwork map, select *File > Open >
Internetwork Map*.

Internetwork Map Display Format

You can display the internetwork map in either of the following
formats:

   ◆ Tree

◆ Connected-graph

Connections in both formats are logical rather than geographic. Figure 2-6 shows part of a sample map in the two formats.

You can switch between the two formats by selecting *Configure > Global Preferences.*

Figure 2-6
Internetwork Map Display Formats

Tree Format

Connected-Graph Format

Connection Reference

Back Link
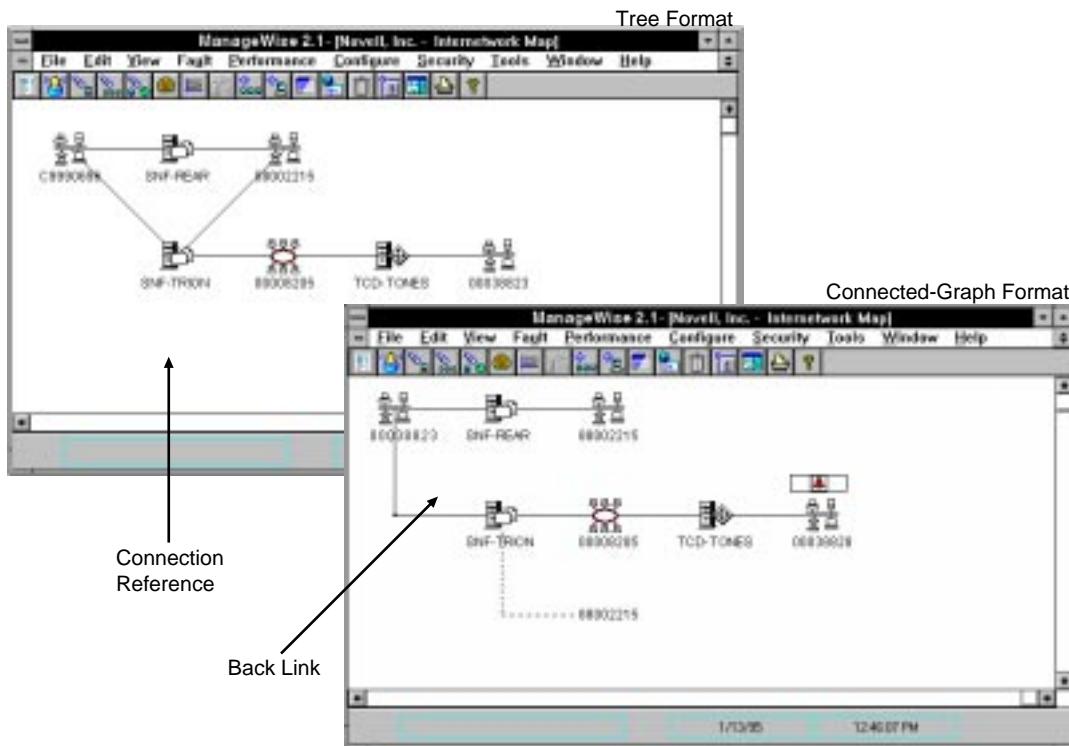
Tree Format

The tree format uses right-angle links and connection references to indicate connections. A connection reference, which is shown by dotted lines, represents a connection between a node and another segment that was drawn earlier and higher in the map. Figure 2-6 shows a

connection reference between the router SNF-TRION and the segment 88002215.

Connected-Graph Format

The connected-graph format uses diagonal links instead of connection references to indicate connections between a node and another node drawn higher in the map. This format is appropriate for small networks of fewer than 20 routers and 20 segments. On a larger map, many links converge on single objects, and links often pass over icons and other links, sometimes giving false impressions of connections.

When you use the connected-graph format, you can move segment and router icons to new positions on the internetwork map. You might want to do so if the layout of the discovered map is hard to read.

Note   If Snap Icons to Grid is set in the Logical Map Options Dialog Page of the Global Preferences dialog box, you can move icons only from one grid to another. This is the default setting. By disabling this option, you can place an icon anywhere on the map.

Changing the Internetwork Map Anchor

Note   When moving icons in the connected-graph format, you can either place icons anywhere on the map or place icons using a grid.

You can change the layout of the internetwork map by specifying a new map *anchor*. An anchor is the object that is displayed in the upper-left corner of the map; all network interconnection is shown as starting from that object. The default anchor is the segment that includes the NetExplorer Server. If your NetExplorer Server is not in the database, the segment with the most LAN components becomes the anchor.

Note   If you want your backbone to appear in the upper left corner of the internetwork map, either make one of the server's on that segment a NetExplorer Server or click the Find Segment action bar button (or select *View > Find > Segment*) to find your backbone and use the Anchor action bar button.

Newly discovered internetwork objects are placed at the bottom of the internetwork map.

In some situations, you might change the anchor to create a map layout that is easier to use. For example, if you repeatedly work with nodes

connected to a specific segment, you might find it more convenient if that segment were the anchor.

To change the anchor, follow these steps:

Procedure

1. **On the map, select the object you want to use as the anchor.**

2. **Click the Set Anchor action bar button.**

   ManageWise redraws the map, placing the icon for the selected object in the upper-left corner. If you are using the tree format of the internetwork map, ManageWise redraws the map and creates new connection references, as illustrated in Figure 2-7.

Note   When you click the Set Anchor action bar button, the new anchor position is saved automatically. The next time you start ManageWise and open the map, the object is displayed in the anchor position.

**Figure 2-7
Changing the Anchor of an Internetwork Map
in the Tree Format**
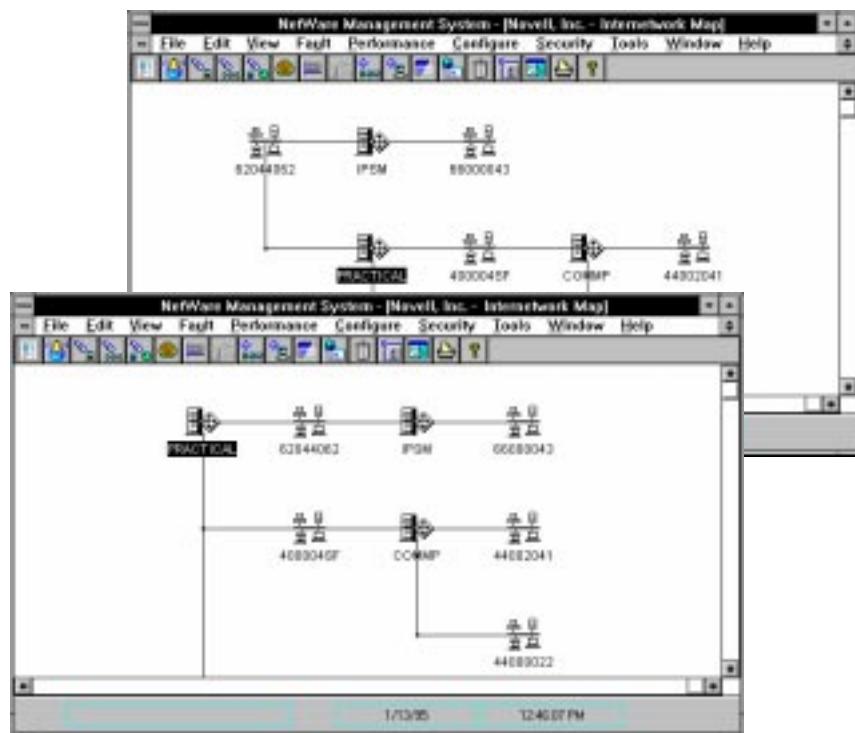
Viewing Segment Maps

ManageWise builds a segment map for each segment shown on the internetwork map (see Figure 2-8).

Figure 2-8
Sample Segment Map
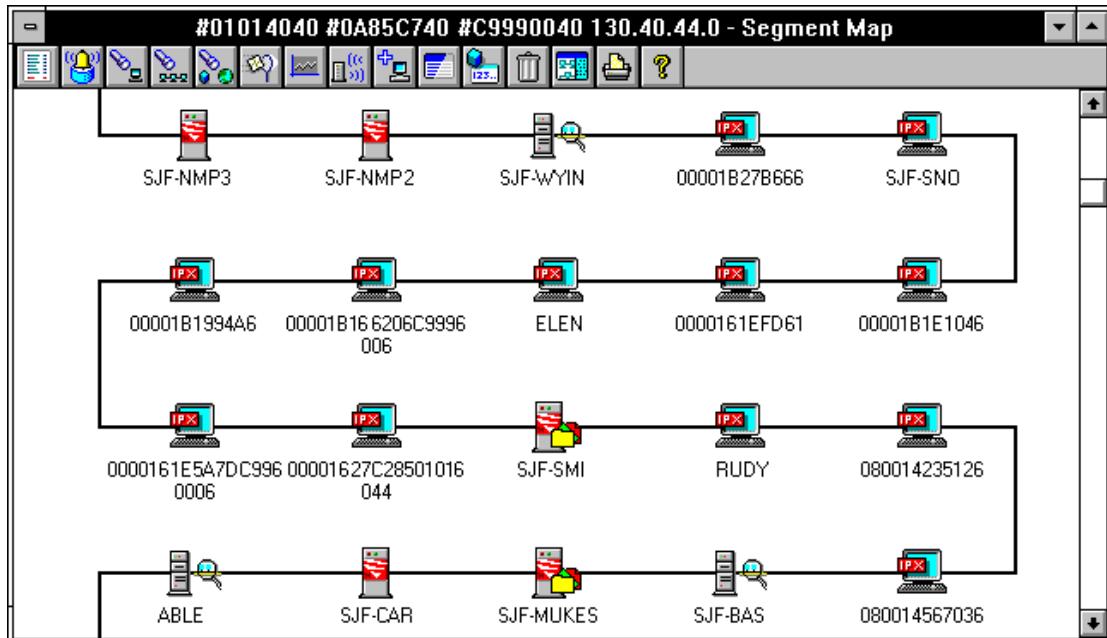
When a segment carries both IP and IPX traffic, the segment name is a concatenation of all the IP and IPX network numbers, separated by a space. For example, a segment can have an address consisting of two IPX addresses and an IP address:

```
#01014197 #010257FF 10.57.44.0
```

You can open a segment map in the following ways:

◆ Double-click the icon for the segment in an open internetwork map.

◆ Select the segment icon in an open internetwork map and select
  File > Open > Segment Map.

◆ Open the segment by name.

By default, the internetwork map remains open when you open one of its segment maps.

After a segment map is open, you can reorder the nodes on the map by object type; name; or MAC address, IP address, or IPX address. (Refer to "Rearranging Nodes on a Segment Map" on this page.)

Segment Map Icons

A segment map includes icons for all objects in the database that are on that segment (routers, workstations, and so on). Each router is displayed on the internetwork map and on each of the segment maps for all segments it connects.

Rearranging Nodes on a Segment Map

You can change the order in which nodes are displayed on a segment map. You can order them by these attributes:

◆ Object type (refer to "Ordering Nodes by Object Type" on page 37)

◆ Name or MAC address, IP address, or IPX address (refer to "Ordering Nodes by Name or Address" on page 38)

You can also arrange nodes on a segment map by using a "drag-and-drop" technique (refer to "Ordering Nodes by Dragging and Dropping" on page 39).

Note ▼ Using the drag-and-drop technique temporarily arranges nodes on a segment map. The arrangements are lost when you close the segment map.

Ordering Nodes by Object Type

To order objects by type on segment maps, specify the order in the Selection List of a dialog box. The order of object types in the Selection List determines the order of appearance in the segment map. You delete objects from the current Selection List or add objects to the Selection List until the order suits your need. When you add an object type to the Selection List, it goes to the bottom of the list.

To order nodes by object type, follow these steps:
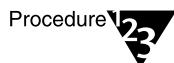
Procedure ▼ **1. Select *View > Arrange By > Object Type*.**

ManageWise displays the Arrange Objects By Type dialog box.
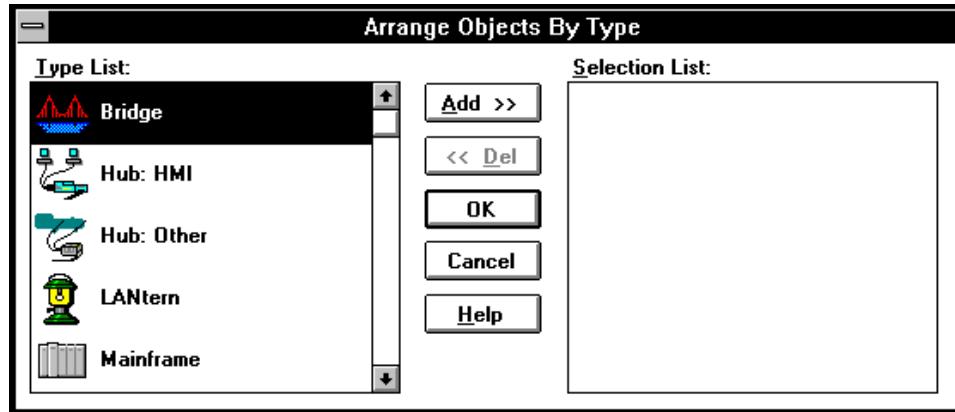
2. **Select an object type from the Type List and click Add, or select an object type from the Selection List and click Del.**

   Alternatively, you can double-click the icon to add or delete an icon to or from the Selection List.

   An added object type moves from the Type List to the bottom of the Selection List or from the Selection List to the Type List.

3. **Repeat Step 2 until you have specified the order you want.**

4. **Click OK.**

   Objects for any types that are not on the Selection List are displayed, in random order, at the end of the map.

Ordering Nodes by Name or Address

You can arrange nodes alphabetically by name or numerically by MAC address or IPX address. To order nodes in these ways, select one of the following commands:

◆ *View > Arrange By > Name* sorts the nodes alphabetically by name in ascending order.

◆ *View > Arrange By > MAC* sorts the nodes numerically by LAN board address in ascending order.

◆ *View > Arrange By > IP* sorts the nodes numerically by IP address in ascending order.

◆ *View > Arrange By > IPX* sorts the nodes numerically by IPX address in ascending order.

Ordering Nodes by Dragging and Dropping

Rearranging nodes by dragging and dropping them on a segment map is not a permanent operation. If you close a segment map after arranging nodes using this technique, then open the same segment map again, the nodes appear as they did before you arranged them.

To arrange nodes by dragging and dropping, follow these steps:

Procedure

1. **Open a segment map.**

2. **Click and hold down the mouse button on a node that you want to move.**

3. **Move the node to a new location on the segment map.**

4. **Release the mouse button.**

   The node moves to the new location.

Displaying Selected Objects on a Segment Map

At times, you might be interested in only certain types of network nodes. You can limit nodes displayed on a segment map by *filtering* them by these attributes:

◆ Object type (refer to "Filtering Objects by Type")

◆ Protocol (refer to "Filtering Objects by Protocol" on page 40)

Filtering Objects by Type

To filter objects by type, follow these steps:

Procedure

1. **Select *View > Filter By > Object Type*.**

   ManageWise displays the Filter Objects By Type dialog box, which lets you select object types to include or exclude from the map.

2. **Select or deselect the Hide check box, as desired.**

The Hide check box determines whether the object types you select are shown on the segment map. If you select the Hide check box, only the object types you select are hidden. Conversely, if you deselect the Hide check box, only the object types you select are shown.

3. **Select an object type from the Type List and click Add.**

Alternatively, double-click the object type from the Type List. The object type icon moves from the Type List to the Selection List.

4. **Repeat Step 3 until you have specified all the objects you want.**

5. **Click OK.**

Filtering Objects by Protocol

To limit objects by IP or IPX protocol, be sure the segment map you want to affect is the active window, then follow these steps:

Procedure

1. **Select *View > Filter By > Protocol*.**

ManageWise displays the Filter Objects By Protocol dialog box, which lets you select protocols to include or exclude from the map.

2. **Select or deselect the Hide check box, as desired.**

The Hide check box determines whether the protocol you select is shown on the segment map. If you select the Hide check box, the

protocol you select is hidden. Conversely, if you deselect the Hide check box, the protocol you select is shown.

3. **Select a protocol from the Protocol List and click Add.**

   Alternatively, double-click the protocol from the Protocol List. The object type icon moves from the Protocol List to the Selection List.

4. **Repeat Step 3 until you have specified all the objects you want.**

5. **Click OK.**

Restoring Filtered Objects to the Map

You can restore filtered objects in these ways:

◆ Turn off the filtering. The restored objects appear at the end of the map.

◆ Close and reopen the segment. The restored objects appear in random order on the map.

Creating Custom Maps

Custom maps let you represent a personal view of your network. You can, for example, represent the location of networks, segments, and nodes relative to your geographic locations. Alternatively, you can create a map that shows only the servers and routers you monitor daily. Custom maps also let you specify the connection between logical networks (represented by the internetwork and segment maps) and physical networks.

This section discusses the following main custom map tasks:

◆ Creating or modifying custom maps

◆ Copying nodes to custom maps

◆ Linking custom maps to each other and to segment maps

Before discussing these tasks, it is important to explain the Custom Map Editor window.

Custom Map Editor Window

The Custom Map Editor window is displayed when you select *Edit > Custom Map > New* to create a custom map. You can also switch easily between the map window and the Editor window on an existing custom map. Click the Edit button in the map window to open the Editor. Click the Exit button in the Editor window to save your changes and return to viewing the map.

The status bar, at the bottom of the window, displays the following from left to right:

◆ Modes of operation, as follows:

  ◆ **Edit**—Enables you to add objects, such as wallpaper, icons, or labels, to the map. This is the default mode.

  ◆ **Resize**—Resizes the wallpaper, the background graphic of a custom map. To enter Resize mode, click the wallpaper (away from any icon or label) to select it. Black squares, called *handles*, appear at the corners and the center of each side. Click a handle and drag it to resize the wallpaper.

  ◆ **Drag**—Enables you to move an object, including the wallpaper, to a new area of the map. To enter Drag mode, click the object you want to move to select it. Then click again, holding down the mouse button, and drag the object to the desired location.

Note ▼ Icons and labels are placed with respect to the map, not the wallpaper. When you drag the wallpaper to a new location, the icons and labels do not move, and their relationship to the wallpaper changes.

◆ Cursor position

◆ Current position of the selected object

You cannot place icons from other maps on your custom map until you save your changes and exit the Custom Map Editor window.

Creating a Custom Map

You can create custom maps that represent such geographic entities as your state, region, city, campus, floor plan, or any other entity for which you have a scanned or drawn bitmap file.

1. Select _Edit > Custom Map > New_.

ManageWise displays the Custom Map Editor window. Refer to "Custom Map Editor Window" on page 42.

2. Click the Wallpaper action bar button.

ManageWise displays the Browse dialog box, which lists bitmap files.

3. Using the Browse dialog box, select a bitmap file.

4. Double-click the file you want to use.

ManageWise displays the Custom Map Editor window again.

5. Click the region of the window where you want to place the center of the map.

The window displays the map with the new wallpaper.

6. Click the Icon Palette action bar button.

ManageWise displays the icon palette.

7. Click a button on the icon palette to create an icon for a city, country, region, or whatever you want.

If the icon you need is not present, click the arrow in the top-right corner of the icon palette to see additional icons.

ManageWise displays the Enter Location Label dialog box.

8. Type the name of the location, and then click OK.

9. Click the area of the map where you want to place the icon.

ManageWise displays the map with the new icon.

10. Click the Exit action bar button.

The Custom Map Editor prompts you to save the map changes before you exit.

11. Click Yes.

ManageWise displays the Enter Page Name dialog box.

12. Type the name of the map as you want it to appear in the list box for *File > Open > Custom Map*.

Repeated use of this procedure creates a map such as the one in Figure 2-9, which displays the map of the United States with specific cities shown. Each of the icons on the map can be linked to other, more specific custom maps.

Figure 2-9
Sample Custom Map
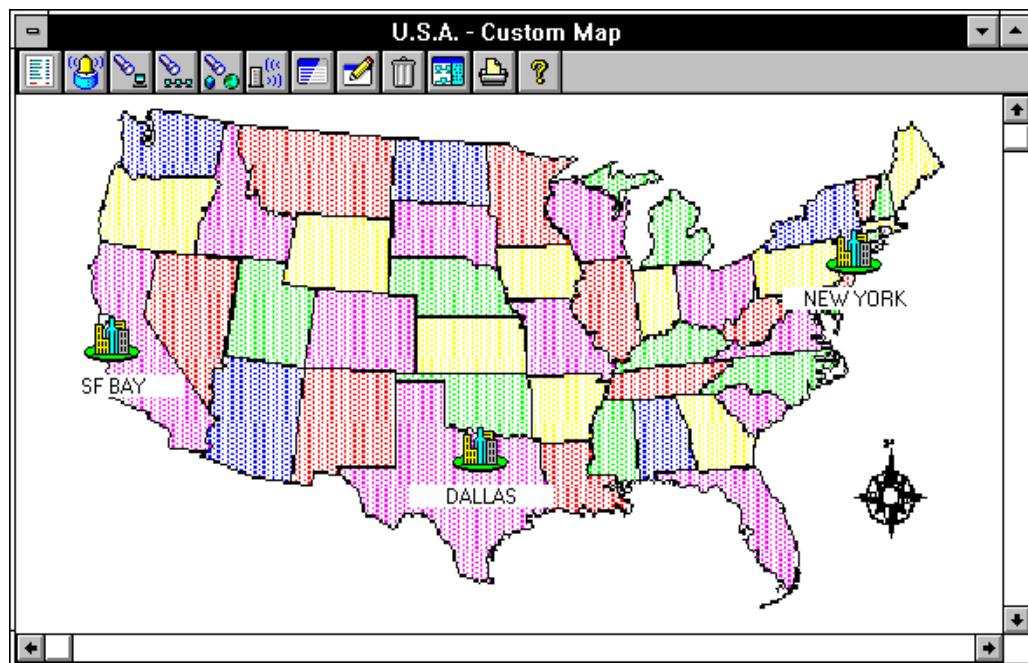
You can rename custom maps by selecting *Edit > Custom Map > Rename*. To edit custom maps, select *Edit > Custom Map > Edit*. To delete custom maps, select *Edit > Custom Map > Delete*.

Copying Nodes to Custom Maps

You can copy nodes from the internetwork map, a segment map, or a custom map to a custom map. For example, you can copy a server to a part of a floor plan custom map that represents an office in a building.

When you copy nodes to a custom map, the node icon is displayed in both maps. Any segment or node alarms that appear on a segment map, the internetwork map, or custom map also appear on the custom map.

To copy a node from a map to a custom map, follow these steps:

Procedure

1. **Open both the custom map and the source map.**

   This procedure does not work if your custom map is in the Custom Map Editor. If you are using the Custom Map Editor, exit and save the map as a custom map.

2. **Select a node icon on the source map.**

3. **Hold down the left mouse button and drag the icon to the custom map, positioning it where you want it to appear.**

Note

The icon representing that node now appears on both the logical map and the custom map. Alarms that affect that node appear on both maps. Double-clicking the node icon has the same effect on both maps.

Linking Custom Maps

You can link custom maps with each other so that double-clicking an icon on one custom map opens another custom map. For example, you can design your map so double-clicking a building icon opens the custom map representing one of the floor plans.

After you link a custom map, alarms propagate throughout the maps. This can be extremely useful for monitoring and troubleshooting. For example, suppose you place several nodes on your building map, which is linked to the building icon on your San Jose map, which is linked to the San Jose icon on your U.S. map. When an alarm is displayed on the U.S. map next to the San Jose icon, you can either click the San Jose icon and click each succeeding icon where an alarm icon is displayed until you find the source of the alarm, or you can select the San Jose icon and click the Alarm Report action bar button to view an alarm report.

To link a location icon on a custom map to another custom map, follow these steps:

1. **Create the custom maps you want to link, as described in the section "Creating a Custom Map" on page 42.**

   You must give unique names to the maps and make sure that you place on one map the icon you want to link to the other map.

2. **Select *File > Open > Custom Map* to open the custom map on which the icon is placed.**

3. **Double-click the icon you want to link to another custom map.**

   Alternatively, you can select *Edit > Custom Map > Link*.

   ManageWise displays the Link dialog box. It lists the custom maps you have created and saved.

   ```
   ┌──────────────────────────────────────┐
   │ ▬              Link                   │
   ├──────────────────────────────────────┤
   │ Map Name:                   ┌───────┐ │
   │                             │  OK   │ │
   │ << New-Page >>              └───────┘ │
   │ BayArea                     ┌───────┐ │
   │ gardineroffice              │Cancel │ │
   │ nwoffices                   └───────┘ │
   │ Provo,bldg1,1stfloor                  │
   │ seattleoffice                         │
   │ usacities                   ┌───────┐ │
   │                             │ Help  │ │
   │                             └───────┘ │
   └──────────────────────────────────────┘
   ```
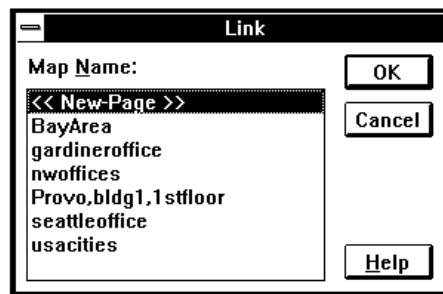
4. **Click the map name (sometimes called "map page") you want to link to the icon.**

   If you did not create a custom map to which you can link, select New-Page. New-Page opens the Custom Map Editor, enabling you to create a custom map. ManageWise links the newly created map after you finish editing it.

5. **Click OK.**

   ManageWise displays both maps.

Adding GoTo Symbols

GoTo symbols are pointers to other maps, rather than links. GoTo symbols are useful when you have a series of linked maps and you want to reference back to a previously linked map. In this situation, a circular reference, you cannot use a link because links cannot be circular. You must use a GoTo symbol.

For example, you have a series of custom maps linked together: USA is linked to CA, which is linked to SAN JOSE, which is linked to BLDG 10, which is linked to ENG SEGMENT. On ENG SEGMENT, you might want to be able to jump to the USA custom map using a double-click. You want to add an icon for that quick reference but you cannot add a link because that would create a circular link (the end referring back to the beginning). ManageWise does not allow circular links. Instead of a link, you add a GoTo icon and point to the USA custom map.

Using the GoTo action bar button, you can point to another custom map, a segment map, or an internetwork map. Because GoTo symbols point to other maps instead of linking to them, alarms do not propagate. To point to another map using the GoTo action bar button, follow these steps:

Procedure

1. **Open the Custom Map Editor on the custom map on which you want the GoTo symbol by clicking the Custom Map Editor action bar button.**

    Alternatively, you can select *Edit > Custom Map > Edit.*

2. **Click the GoTo action bar button.**

    The Select Target Map dialog box appears.

3. **Select the desired map type from the list box.**

    You can select a custom map, segment map, or internetwork map. Depending on the map type, the map name list box shows custom map names, segment names, or internetwork map names.

4. **Click the name of the map to which you want the custom map to point.**

5. **Click OK.**

    The dialog box disappears and the pointer changes from an arrow to a pointing hand.

6. **Place the icon on the custom map.**

   Position the icon using the mouse and place it by clicking the left mouse button. The icon can be repositioned by clicking the icon and moving the mouse while holding down the left mouse button.

7. **Click the Exit action bar button.**

   The Custom Map Editor prompts you to save the map changes before you exit.

8. **Click Yes.**

   ManageWise displays the custom map. When you double-click the hand icon, the map pointed to by the GoTo symbol appears.

c h a p t e r **3** *Tailoring Maps and Object Data*

ManageWise® software creates maps according to what NetExplorer™
software discovers. Occasionally, NetExplorer finds a router that cannot
be discovered fully. When this happens, ManageWise generates an
incomplete map from the discovery data. To tailor the map to more
accurately portray your network, you might want to change the way
objects are configured, add objects to a map, or delete objects from it.
The following sections describe ways you can tailor maps to suit your
needs.

Note ▼ The changes you make affect the way the map is displayed and also affect the
database. They do not affect the network.

Changing Object Information

NetExplorer collects a wide variety of data, which you can edit or to
which you can add other information. For example, NetExplorer
collects the following information about workstations:

◆ Name

◆ Object type (such as PC)

◆ Network and MAC addresses

Using the Database Object Editor, you can add to the NetExplorer data
to make your records more complete. For example, you can add
workstation location information—such as office, floor, building,
campus, city, region, state, and country—to the database.

You can store useful configuration information in the ManageWise
database. This information can help you manage your inventory, track
service, and know who to call when a node has a problem. You can
protect this information with a password. You must use the password
to change the information about your network nodes.

You can also edit data that you or NetExplorer create. You can change data to reflect your own preferences or to correct it. For example, you can change the name of a workstation. Similarly, if NetExplorer combines a number of segments as one, you can edit the database and reconstruct that part of the map to reflect your network topology accurately.

Note ▼ Editing the data affects the database but not the actual hardware. In some instances, editing can also affect ManageWise operations. For example, if you change the address of a server to an incorrect address, ManageWise cannot contact the server until you run NetExplorer or correct the mistake manually.

Using the Database Object Editor

The ManageWise Database Object Editor enables you to view and edit object configuration information. The Editor displays two different sets of information, one for nodes and one for segments. The Editor displays the information in a series of "pages." Each series begins with a Configuration Summary page. Figure 3-1 shows the first page in the node Editor.

To display or change the database information about a segment or node, follow these steps:

Procedure ▼ **1. Select the object on an internetwork map, a segment map, or in a list window such as the NetWare Servers window or Routers window.**

2. Select *Edit > Database Object*.

Alternatively, you can click the Edit Object action bar button.

The system displays the Database Object Editor with the Configuration Summary for the object, as appropriate to segments or to nodes.

For example, in Figure 3-1, the Editor presents information about a server with the name SJF-ATHEN.

Figure 3-1
**Sample First Page
of Database Object
Editor**

If you want to make changes or examine and edit more detailed
information, go to the next step. Otherwise, you can close the
window or print the dialog box using the appropriate button.

Note The Print Summary button on the Configuration Summary dialog page
prints a summary of information about the selected object. The other dialog
pages you can select have a Print button that only prints a picture of the
dialog page.

**3. Select the desired icon from the column on the right side of the
dialog box.**

The icon represents the type of information you want to display or
change. The following is a list of procedures for changing the
information represented by the icons:

◆ "Changing the Node Icon" on page 53

◆ "Adding Services" on page 54

◆ "Editing Adapter Information" on page 55

◆ "Changing the Node or Segment Name" on page 57

◆ "Listing the Make and Model of Your System" on page 57

◆ "Listing Disk Information of a Node" on page 58

◆ "Listing Contact Information" on page 59

◆ "Listing Locational Information" on page 60

- ◆ "Listing Miscellaneous Information" on page 60

- ◆ "Editing Segment Information" on page 61

- ◆ "Choosing a Remote Monitor" on page 61

- ◆ "Enabling and Disabling Segment Alarms" on page 62

4. **Change or add information.**

   The system displays appropriate Add dialog boxes. Add the information, and then click OK.

5. **Click the Save button, if one appears on the dialog box.**

   If you switch from one page to another or attempt to close the Database Object Editor without saving, the message `Save changes first?` appears in a dialog box. Click OK to save the changes.

6. **Repeat Step 3 and Step 4, as needed.**

   Canceling edits to a dialog page does not affect previously saved changes to other dialog pages.

7. **After you complete your changes, close the Database Object Editor by double-clicking the Control-menu box or by clicking the Control-menu box and selecting *Close*.**

   Alternatively, press Alt+F4 to close the Database Object Editor.

Information available in dialog pages differs slightly for nodes and segments:

- ◆ For nodes, the Editor displays pages for a configuration summary and for information about the system, the adapter, services, the disk, individuals to contact, the location of the node, and other miscellaneous information.

- ◆ For segments, the Editor displays pages for a configuration summary and for information about the segment, individuals to contact, servers to monitor, alarms on the segment, and other miscellaneous information.

Note   Third-party products might add more dialog pages to the Database Object Editor or the Global Preferences dialog box.

The following sections provide procedures for adding or editing information to the dialog pages after opening the Database Object Editor. These are procedures that you can perform in Steps 3 and 4 of the preceding procedure.

Changing the Node Icon

You can change the icon that represents a node on a map. This makes it easy for you to identify the function of a particular node by looking at its icon. You can change the icon in the System Information dialog page and the Services dialog page. ManageWise sets the icon for a node if you do not set one.

The ManageWise hierarchy for icons is as follows:

1. Icons set by you in the System Information dialog page

2. Icons set by you in the Services dialog page

3. Icons set by ManageWise

An icon set in the System Information dialog page overrides an icon set in the Services dialog page or one set by ManageWise. An icon set in the Services dialog page overrides only an icon set by ManageWise.

Note ▼ NetExplorer does not change an icon if you set one in the System Information or Services dialog pages.

Change the icon in the System Information dialog page if you want to represent a node with a particular icon, making it easier to identify the node at a glance. To change the icon in the System Information dialog page, follow these steps:

Procedure ▼
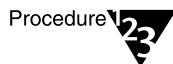
1. **Select the node and open the Database Object Editor.**

2. **Click the System Information icon.**

3. **In the Device Type box, click the Change Icon button.**

   The Change Icon dialog box appears.

4. **Select an icon by scrolling through the listed icons or by selecting an icon bitmap file using the Browse button.**

5. Click OK.

The Change Icon dialog box disappears, and the selected icon appears in the Device Type box.

Change the icon in the Services dialog page if you want to represent a node with an icon that shows a service provided by the node. To change the icon in the Services dialog page, follow these steps:

Procedure ▼

1. Select the node and open the Database Object Editor.

2. Click the Services icon.

3. Select the service you want the icon to represent on maps.

If the service you want to represent is not listed, follow the procedures listed in "Adding Services."

4. Click the Service On Icon button.

5. Click Save.

To show you the service icon used on maps, the words *default icon* follow the chosen service.

Adding Services

The Services dialog page lets you represent services the node provides as icons. To add services to the node, follow these steps:

Procedure ▼

1. Select the node and open the Database Object Editor.

2. Click the Services icon.

The Services dialog page appears on the screen.

3. Click the Edit button.

The Select Services to Add dialog box appears.

4. Select a service from the Available Services column and click Add.

Alternatively, double-click a service from the Available Services column. The service transfers from the Available Services column to the Selected Services column.

Some services require NetWare® File Service in addition to the service you choose (NetWare Management Agent™ software and NetWare LANalyzer® Agent™ software are two examples). When you add a service that requires NetWare File Service, NetWare File Service is automatically added unless it is already there.

Other services require an internal network number—NetWare File Service, for example.

5. Repeat Step 4 for as many services as the node provides.

6. Click OK.

The Services dialog page appears, listing the added services.

The first service selected becomes the default service icon displayed on maps. To change the icon, see "Changing the Node Icon" on page 53.

7. Click Save.

Editing Adapter Information

NetExplorer initially enters information about a node's adapters when it discovers the network or you enter information when you tailor maps (add nodes, connect objects, and so on). In either case, adapter information might be incorrect or missing.

To add information for an adapter that is missing, follow these steps:

Procedure
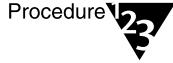
1. Collect information about the adapter's MAC address, protocol, frame type, network address, and the segment to which the node is to be added.

2. Select the node and open the Database Object Editor.

3. Click the Adapter Information icon.

The Adapter Information dialog page appears on the screen.

4. Click the Add button.

The Add One Network Interface dialog box appears.

To edit erroneous adapter information that the Adapter Information dialog box lists, follow Step 2 and Step 3, but instead of clicking the Add button, click the Edit button.

5. Correct the information listed in the Segment Connected to, MAC Address, Protocol, Frame Type, and Network Address edit boxes, or add the information if it does not exist.

6. Set the Prevent Deletion by NetExplorer check box.

This prevents NetExplorer from deleting or updating the binding you corrected.

7. Click Add in the Binding Information box.

The protocol, frame type, and network address appear in the Binding Summary table.

8. Click OK.

The Adapter Information dialog page appears, listing the added network interface.

To add information listed in the Setup Information dialog box, follow these steps:
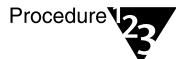
Procedure

1. Collect information about the interface's values for I/O Port and Memory Address Interrupt.

2. Follow Step 2 through Step 4 of the preceding procedure for editing erroneous adapter information.

The Edit Network Interface dialog box appears.

3. Click the Setup button.

The Network Interface Parameters dialog box appears.

4. Enter the interface's values for I/O Port, Memory Address, Interrupt, and select DMA use, if you are using DMA.

5. Click OK.

The Edit Network Interface dialog box reappears.

6. Click OK.

Changing the Node or Segment Name

You can change the name of a node or segment shown on any map. IPX™ network numbers and MAC addresses are used as names if you do not assign a name to a node or segment.

Note Normally, NetExplorer will not change a segment name you entered unless the name begins with a pound sign (#). An exception to this is a token ring segment with NetWare LANalyzer Agent software installed on a server. In this case, the name might change back to the original name if NetExplorer is still discovering your internetwork.

Suggestion Wait until the completion of the first discovery cycle before changing segment names. NetExplorer might run up to three discovery modules during the initial discovery cycle. Refer to "Understanding Discovery Cycles" on page 81 for more information.

To change the name to one that is more meaningful, follow these steps:

Procedure 1. **Select the node and open the Database Object Editor.**

2. **Click the System Information icon (for node) or the Segment Information icon (for segment).**

   The System Information dialog page (for node) or the Segment Information dialog page (for segment) appears.

3. **Enter the new name in the name text box.**

Note Do not use a name that begins with a digit or a pound sign (#).

4. **Click Save.**

Note NetExplorer does not change a name if you set one.

Listing the Make and Model of Your System

You can list the type of computer used as a node. By listing this information, you can document the types of computers used on your network (PC, minicomputer, and so on). To list the make and model of your system, follow these steps:

Procedure 1. **Select the node and open the Database Object Editor.**

2. **Click the System Information icon.**

The System Information dialog page appears.

3. **Click the Add button in the Available Make and Model box.**

The Add System Make and Model dialog box appears.

4. **Enter the make and model information in the appropriate edit box.**

If you have a bitmap picture of the computer, you can add it by entering the filename of the bitmap file in the Picture box, or you can use the Browse button to find the bitmap file.

5. **Click OK.**

The make and model of the computer appear in the Available Make and Model box. The Available Make and Model box lists all the computers used on the network.

6. **Select the make and model that describe this node.**

7. **Click Select in the Make and Model box.**

The make and model appear in the Available Make and Model box. If a picture was added, the Picture button is selectable. Click Picture to see the bitmap picture of the system.

8. **Click Save.**

Listing Disk Information of a Node

You can use ManageWise to document the types and capacities of drives used on each node on your network. To list the type of drive used by a node, follow these steps:

Procedure

1. **Select the node and open the Database Object Editor.**

2. **Click the Disk Information icon.**

The Disk Information dialog page appears.

3. **Click the Add button in the Available Make and Model box.**

The Add Disk Make and Model dialog box appears.

4. **Enter the make and model information and the type of disk in the appropriate edit box.**

5. **Click OK.**

   The make, model, and type of disk appear in the Available Make and Model box. The Available Make and Model box lists all the disks used on the network.

6. **Select the make and model that describe the hard disk used by this node in the Available Make and Model box.**

   After selecting the make and model of hard disk, the Add button in the Disk Information box is selectable.

7. **Click Add in the Disk Information box.**

   The make and model appear in the Disk Information box.

8. **Click Save.**

Listing Contact Information

You can list a person or persons to contact if something happens to a node or segment on your network. To list contacts, follow these steps:

Procedure

1. **Select the node and open the Database Object Editor.**

2. **Click the Contact Information icon.**

   The Contact Information dialog page appears.

3. **Click the Add button in the Contact List box.**

   The Add Contact dialog box appears.

4. **Enter information about the contact in the appropriate edit box.**

   If you have a bitmap picture of the person, you can add it by entering the filename of the bitmap file in the Picture box, or you can use the Browse button to find the bitmap file.

5. **Click OK.**

   The contact name appears in the Contact List box. The Contact List box lists contacts for the entire network.

6. **Select the contact for this node or segment.**

   After selecting the contact, the Add button in the Contact Information box is selectable.

7. **Click Add in the Contact Information box.**

   The contact appears in the Contact Information box.

8. **Click Save.**

Listing Locational Information

You can use ManageWise to store the locations of nodes and segments. Then, when tracing an alarm or installing upgrades, you can retrieve the location of the relevant node or segment. To list locations, follow these steps:

Procedure

1. **Select the node and open the Database Object Editor.**

2. **Click the Location Information icon.**

   The Location Information dialog page appears.

3. **Enter information about the location in the appropriate edit box.**

4. **Click Save.**

   The location information appears in this dialog page and in the Configuration Summary dialog page.

Listing Miscellaneous Information

You can list any additional information for a node or segment that you want in the Miscellaneous Information dialog page. To list miscellaneous information, follow these steps:

Procedure

1. **Select the node and open the Database Object Editor.**

2. **Click the Miscellaneous Information icon.**

   The Miscellaneous Information dialog page appears.

3. **Enter any additional information you want about the node or segment.**

4. Click Save.

Editing Segment Information

As with nodes, segment information can be left out during discovery or when you edit the database manually. To add missing segment information, follow these steps:

Procedure **23**

1. Select the node and open the Database Object Editor.

2. Click the Segment Information icon.

The Segment Information dialog page appears.

3. Click Add in the Network Summary box.

The Add Network dialog box appears.

4. Enter a protocol and network address in the appropriate edit box.

5. Click OK.

The information is displayed in the Network Summary table.

6. Click Save.

Choosing a Remote Monitor

Remote monitors, such as NetWare LANalyzer Agent servers, provide information about the segments they are on (refer to Chapter 13, "Analyzing Your Network.") Sometimes the node on which the remote monitor resides must be taken off the network (either for maintenance or because something is wrong with it). When this occurs, you should choose a different remote monitor on the segment to prevent the segment from going unmonitored. To choose a remote monitor, follow these steps:

Procedure **23**

1. Select the node and open the Database Object Editor.

2. Click the LANalyzer Server icon.

A list of nodes running remote monitors on the segment appears. The currently selected remote monitor is highlighted.

3. **Select the node that you want to substitute.**

4. **Click Save.**

Enabling and Disabling Segment Alarms

Remote monitors use segment alarms to monitor Ethernet, token ring and FDDI segments. ManageWise provides segment alarms but does not enable them. Procedures follow for enabling segment alarms, changing thresholds for enabled segment alarms, and disabling segment alarms.

To enable alarms for a segment, set alarm thresholds, or both, follow these steps:

Procedure

1. **Select the node and open the Database Object Editor.**

2. **Click the Segment Alarms icon.**

   The Segment Alarms dialog box appears. The dialog box shows either Ethernet, token ring, or FDDI statistics, depending on the segment. Initially, all alarms are disabled.

   To enable all alarms, go to the next step. To enable an alarm for a single statistic, go to Step 4.

3. **To enable all alarms and use the default threshold and sampling interval values, click Default All.**

   Default values appear in the Threshold and Sampling (sec) columns.

4. **To enable an alarm for a single statistic and set a threshold and sampling interval, double-click the statistic, or select it and click Edit.**

   The Set Alarm dialog box appears for the statistic you chose.

Note

To use the default value for threshold and sample interval, click Default.

   4a. **Enter a threshold in the Value text box.**

   4b. **Enter a time period in the Sample Interval text box.**

       This is the time period over which you want NetWare LANalyzer Agent to average the statistic.

4c.   Click OK.

4d.   Repeat Step 4a through Step 4c if you want to enable additional alarms or set additional thresholds.

5. Click Save.

To disable alarms for a segment, follow these steps after selecting a monitored segment and opening the Database Object Editor:

Procedure ▼ 23

1. Click the Segment Alarms icon.

The Segment Alarms dialog box appears. The dialog box shows either Ethernet, token ring, or FDDI statistics, depending on the segment. Initially, all alarms are disabled.

To disable all alarms, go to the next step. To disable an alarm for a single statistic, go to Step 3.

2. To disable all alarms, click Disable.

Default values appear in the Threshold and Sampling (sec) columns.

3. To disable a single alarm, follow these steps:

3a.   Double-click the statistic, or select it and click Edit.

The Set Alarm dialog box appears for the statistic you chose.

3b.   Click Disable.

3c.   Repeat Step 3a and Step 3b for all alarms you want to disable.

4. Click Save.

Adding and Deleting Objects

When you open an internetwork map or segment the first time, you might find that some segments or nodes are missing or misplaced. This can happen if NetExplorer does not discover objects or consolidates segments when you do not want them consolidated. By adding and deleting objects, you can edit the internetwork map or segment maps to correct any discovery mishaps.

You can create the internetwork map without using NetExplorer. This procedure is outlined in "Creating Maps without NetExplorer" on page 72. "Troubleshooting Maps" on page 73 lists a number of different situations in which you add objects, delete objects, or do both to create an accurate map.

Adding Objects to Maps and to the Database

As you work in ManageWise, you might want to add objects to your maps and to the database. For example, if ManageWise does not discover an object, you might want to add it manually. You can add either segments or nodes to your maps manually. To make adding an object easier, collect the following information before adding a node or segment:

♦ If adding a node, the segment to which the node is added.

♦ If adding a node, the frame type used by the node.

♦ If adding a node, the MAC address for the node (one MAC address for each network interface.

♦ The network protocol used (TCP/IP, IPX, OSI, and so on). If you are using TCP/IP, you might have to include a subnet mask.

Adding Segments

To add a segment to the internetwork map, follow these steps:

Procedure
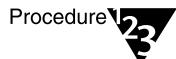
1. Open the internetwork map.

If your internetwork map is empty, ManageWise enables you to add a segment to start the map.

2. Select *Edit > Add > Segment*, or click the Add Segment button on the action bar.

ManageWise displays the Add One New Segment dialog box, shown in Figure 3-2.

Figure 3-2
Add One New
Segment Dialog Box

3. Select the type of segment you want to add.

For example, in Figure 3-2, a WAN: Dialup segment is being added.

4. Click OK.

ManageWise displays a dialog box in which you can enter basic information about the segment. For example, Figure 3-3 shows the Add One WAN: Dialup Segment dialog box.

Figure 3-3
Add One Segment
Information Dialog
Box
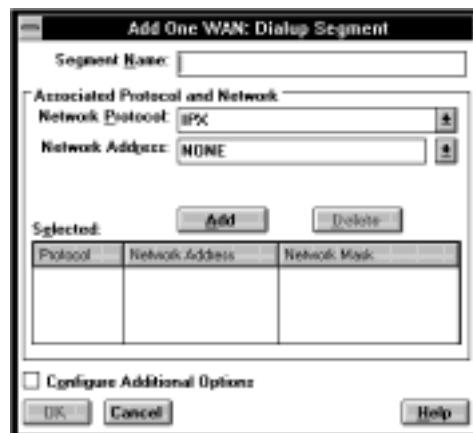
5. **Fill in the Add One Segment Information dialog box with the segment name, protocol, network address, and network mask (for IP protocol only) information.**

   NetExplorer does not change the segment name that you enter.

   Note ▼ Wait until the first discovery cycle is complete before changing segment names. Refer to "Understanding Discovery Cycles" on page 81 for more information.

   If the protocol for the added segment is IP, the Network Mask field appears in the dialog box. You can add a subnet mask to further specify your segment.

   If the protocol for the added segment is IPX, a text string NONE is included in the Network Address list box. Select NONE to specify an IPX unnumbered segment for a WAN link.

   If the protocol you select from the list is something other than IP or IPX (SNA, for example), the network address is for informational purposes only (the Network Address list box becomes a text field).

6. **Click Add to implement the chosen protocol and network address.**

7. **If you want to add more information about the segment, such as cable types or contact information, click the Configure Additional Options check box.**

   Selecting this check box causes ManageWise to open the Database Object Editor after adding the segment.

8. **Click OK.**

   ManageWise adds the segment and redraws the internetwork map.

Adding a Node

A segment must be in the ManageWise database before you can add a node to it. You can add a node to either the internetwork map or a segment map. To add a node, follow these steps:
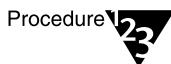
Procedure ▼ 1. **Open the internetwork map and select the segment to which the new node should be connected.**

   Alternatively, open the segment map of the segment to which the new node should be connected.

The segment you select is the default segment. You are given an opportunity to change the segment later in the procedure (refer to Step 7b on page 69).

2. **Select *Edit > Add > Node*, or click the Add Node action bar button.**

   ManageWise displays the Add One New Node dialog box, shown in Figure 3-4.

Figure 3-4
Add One New Node
Dialog Box

3. **Select the type of node you want to add from the list.**

   In Figure 3-4, a NetWare File Server is being added. The type of node you select should represent the service you see the node providing. This determines the icon ManageWise displays on the map. If the node provides multiple services—for example, if your file server is also a router and a printer server—you can add them later in the process. You can also latch a specific icon to the node, one that allows you to identify the node quickly. Refer to "Changing the Node Icon" on page 53 for more information.

4. **Click OK.**

   ManageWise displays a dialog box in which you can enter basic information about the node. For example, Figure 3-5 shows the Add One NetWare File Server dialog box.

Figure 3-5
Add One NetWare
File Server Dialog
Box

5. **In the System Name field, enter the name you want to give the node.**

   If the service or services selected requires you to add an IPX internal network number, a NetWare File Server, for example, the IPX internal network number must be unique in the entire database.

   Note ▼ If the internal network number you add is a duplicate of one in the database, a dialog box appears when you try to add the node, informing you that you must change the internal network number.

6. **If you want to add additional services to the node, click the Edit button next to the words Services of This Node.**

   Refer to "Adding Services" on page 54 for more information.

7. **Add information about your node's network interfaces:**

   7a. **Click Add.**

   The Add One Network Interface dialog box appears.

Figure 3-6
Segment Connected to List Box

```
╔═══════════════════════════════════════════════════════╗
║ ▬         Add One Network Interface                   ║
╠═══════════════════════════════════════════════════════╣
║ Segment Connected to: │#01014044 #0A85C743 #C9990006 13│ ▼ ║
║                                                         ║
║        Make and Model: │                            │ ▼ ║
║                                                         ║
║          MAC Address: │00│-│00│-│00│-│00│-│00│-│00│    ║
║ ┌─Binding Information────────────────────────────────┐ ║
║ │            Protocol: │IPX                    │ ▼    │ ║
║ │                                                     │ ║
║ │          Frame Type: │ETHERNET 802.2         │ ▼    │ ║
║ │                                                     │ ║
║ │      Network Address: │01014044   │ ▼ │: 000000000000│ ║
║ │        Prevent Deletion By NetExplorer ⊠           │ ║
║ │ Binding Summary:     │   Add   │    │  Delete  │    │ ║
║ │ ┌──────────────┬────────────┬──────────┬─────────┐ │ ║
║ │ │Network Address│ Frame Type │ Protocol │Prevent Deletion│║
║ │ │              │            │          │         │ │ ║
║ │ │              │            │          │         │ │ ║
║ │ │              │            │          │         │ │ ║
║ │ │              │            │          │         │ │ ║
║ │ └──────────────┴────────────┴──────────┴─────────┘ │ ║
║ └─────────────────────────────────────────────────────┘║
║ │  OK  │  │ Cancel │  │ Setup... │         │  Help  │   ║
╚═══════════════════════════════════════════════════════╝
```
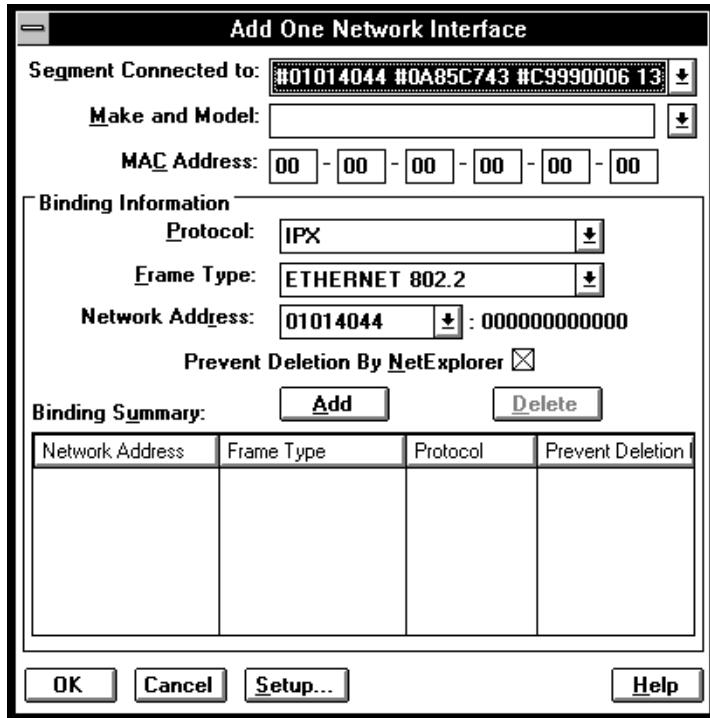
7b. In the Segment Connected to list box, select the segment to which you want the node connected.

ManageWise determines the default selection by the active window from which the Add Node process began. If the active window is a segment map, the default selection is the segment. If the active window is the internetwork map, the default selection is either the segment you previously selected in the internetwork map or, if you did not select a segment, the first segment entry in the Segment Connected to list box.

Segments are listed using either regular text or gray text. Segments listed using regular text are segments that are compatible with the binding. A segment is compatible with the current set of bindings if one of the networks running on the segment meets one of the following:

◆ For an IPX address—every IPX address of the network interface's binding is the same as the IPX address of one of the network's running on the segment.

◆ For an IP address—every IP address of the binding is on one of the IP subnets running on the segment.

◆ For any other type of network—Protocol used by the network interface matches that of one of the networks running on the segment.

Segments listed using gray text are segments that are not compatible with the binding. If you select a segment from the list that is not compatible with the binding, a dialog box appears. From the dialog box, you can either proceed with the segment change and delete the current bindings listed, or you can cancel the selection to the new segment.

7c. Add the MAC address of the network interface you want to connect.

The default value for a new network interface is 00-00-00-00-00-00. For a network interface that does not have a MAC address, leave the MAC address as is. The MAC address entered must be unique to the entire database, except in the case of all zeros.

If you want to override this requirement (for example, if you want to specify MAC addresses from one manufacturer as special MAC addresses), you must add the duplicate address in the NMS.INI file under the [NETEXPLORER] section (refer to "What to Do if You Want Duplicate MAC Addresses" on page 76).

7d. Add the protocol, frame type, and network address.

Protocols and frame types are listed in their respective list boxes. The network address depends on the protocol used.

◆ IP address—For adding an IP binding, the IP address must reside on one of the IP subnets that runs on the segment, must be unique in the entire database, and the bits that make up the node portion of the address must not be all zeros or all ones.

◆ IPX address—For adding an IPX binding, the IPX address must be chosen from the list of IPX networks that runs on the selected segment.

Note   NetExplorer does not modify or delete your changes if you select the Prevent Deletion By NetExplorer check box.

7e. Click Add.

The MAC address and the segment to which you are connecting the node are listed in the Network Interfaces table. To see the details of a network interface, click Edit.

8. **If you want to add more information about the node, such as adapter and disk types, location, or contact information, or if you want to change the node's icon, select the Configure Additional Options check box.**

9. **Click OK.**

   ManageWise adds the node and redraws the affected map. If you selected the Configure Additional Options check box, the Database Object Editor opens.

Note The OK button is not enabled until you enter a minimum set of valid parameters. These parameters are found in the binding information section of the Add One Network Interface dialog box (refer to Step 7d on page 70).

Deleting Objects

You can delete objects from internetwork, segment, and custom maps. If you are deleting a segment, you are also deleting all the nodes in that segment. Be sure deleting the segment is what you want to do before doing it.

Note Some deletion operations can take some time to complete. For example, deleting a segment containing many objects can take 45 seconds or more to complete.

Important When you delete a node (workstation, server, router, bridge, and so on) from an internetwork or segment map or a segment from the internetwork map, the object or segment is deleted from all maps and from the database.

There are two ways to add an object or segment back to the internetwork or segment map after deleting it. You can run NetExplorer and rediscover the network (refer to "Starting NetExplorer Manager Manually" on page 91), or select *Edit > Add > Node* (refer to "Adding a Node" on page 66), or select *Edit > Add > Segment* (refer to "Adding Segments" on page 64).

You can delete objects from a custom map or from the Custom Map Editor (refer to "Custom Map Editor Window" on page 42).

Note When you delete an object from a custom map, the object is removed from that map only. It remains in the database and on all other maps, including any other custom maps to which you have copied it.

Moving Nodes from Segment Map to Segment Map

There are two situations in which you can move nodes from one segment to another:

◆ When the two segments have the same network protocols and network numbers (between two bridged segments, for example; refer to "What to Do if You Have Bridged Segments" on page 73).

◆ When you are moving nodes from the LOCATION UNKNOWN segment to other segments.

Creating Maps without NetExplorer

Initially, ManageWise has an empty internetwork map. You can populate this map yourself if you choose, without running NetExplorer and NetExplorer Manager.

To populate your maps manually, follow these steps:

Procedure **1. Collect information that describes your network.**

Collect information such as names and addresses of routers and bridges, addresses of segments, and addresses and locations of nodes.

2. Select *File > Open > Internetwork Map* to open the internetwork map.

You receive a message that the map is empty.

3. Add a segment to the empty map, as described in "Adding Segments" on page 64.

ManageWise adds the segment, selects it on the internetwork map, and flashes a box around its icon.

4. Open the new segment map by double-clicking the new segment icon.

5. **Add nodes to the segment map, as described in "Adding a Node" on page 66.**

6. **If you have multiple segments, repeat Step 2 through Step 4 for each segment.**

7. **Return to the internetwork map and add nodes, such as routers or bridges, as needed.**

   Each time you add a router or bridge, select one of the segments it is connected to before adding the node. This causes ManageWise to connect the node to that segment automatically.

Troubleshooting Maps

You might have situations on your network that cause the map created by the discovery process to be incorrect. The following sections outline some of these situations and provide procedures to help you correct your map. If you have problems with your maps that are not addressed in this section, refer to Chapter 5, "Troubleshooting Network Discovery."

What to Do if You Have Bridged Segments

ManageWise discovers only routed segments. The result is that bridged segments are consolidated into one segment on the map. To divide the consolidated segment into the bridge and multiple segments that are actually there, follow these steps:
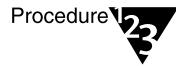
Procedure

1. **Open the segment map for the consolidated segment.**

2. **Add a bridge to the consolidated segment.**

   Follow the procedure in "Adding a Node" on page 66.

3. **Add the rest of the segments to the internetwork map.**

   Follow the procedure in "Adding Segments" on page 64.

Note

The segments that you add must have the same network address and protocol as the consolidated segment.

4. **Add a bridge to the second segment.**

A bridge can be added to the second segment by dragging the
bridge icon from the consolidated segment to the second segment.
To drag the bridge icon, follow these steps:

4a. Click the bridge icon while pressing the Ctrl **key.**

**4b. Move the icon to the second segment map while holding
down the mouse button.**

4c. Release the mouse button.

The Add One Network Interface dialog box appears on the
screen. The network address and protocol shown in the dialog
box is the same as that of the consolidated segment. Do not
change this information.

**4d. Enter the MAC address of the adapter for the second
segment.**

4e. Click OK.

Note The bridge's network interface that you add must have the same network
address and protocol as the consolidated segment.

**5. Move nodes that belong on the second segment from the
consolidated segment to the second segment.**

To move a node, follow these steps:

**5a. Click and hold down the mouse button on a node icon that
you want to move to the second segment.**

**5b. Move the icon from the consolidated segment to the
second segment.**

5c. Release the mouse button.

The icon moves from the consolidated segment to the second
segment.

**5d. Repeat Step 5a through Step 5c until you move all the
node icons that belong on the second segment.**

Alternatively, click nodes while pressing the Shift key to select a
number of nodes. Then, follow Step 5b and Step 5c to move them
all.

**6. If you have multiple bridged segments, repeat Step 1 through
Step 5 for every bridged segment.**

Note ▼ NetExplorer does not move the nodes on the second segment back to the original segment.

What to Do if You Have Segment Islands

The internetwork map sometimes includes objects that are not connected to the main map. These "segment islands" appear at the end of the map, ordered by decreasing size. These islands might involve a third-party router, such as a Cisco or Bay Networks router, or occur when discovery is not yet complete.

If you know that an island is actually connected to another part of the map, you can add a line or connection reference that represents an internetwork connection between a segment and a router, bridge, or brouter. Connection references are discussed in "Internetwork Map Display Format" on page 31.

To represent the missing connection, follow these steps:
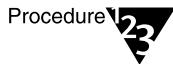
Procedure ▼ 1. **Select the segment and the connecting object.**

To select both, click both objects while pressing the Shift key.

2. **Select *Edit > Connect Objects*.**

The Add One Network Interface dialog box appears on the screen. The protocol and network address information shown in the dialog box are that of the island.

3. **Click the Add button to add the address and protocol to the binding summary.**

4. **Enter the MAC address for the interface adapter.**

5. **Click OK.**

ManageWise updates the internetwork map. Similarly, you can delete a link by selecting the appropriate connecting object and segment and selecting *Edit > Disconnect Objects*.

What to Do if You Have Undiscovered Network Nodes

NetExplorer discovers only IPX objects and IP routers. So, for example, you might want to add to your maps those mainframes, UNIX*

workstations, and other objects that were not discovered. To add objects that NetExplorer did not discover, follow the procedures listed in "Adding a Node" on page 66.

What to Do if You Have an Unusual Network

You might have an unusual network. If this is the case, you might not want to run NetExplorer and NetExplorer Manager. In this situation you can add your entire network, beginning with a segment and then proceeding to add devices to the segment. To do this, follow the steps listed in "Creating Maps without NetExplorer" on page 72.

What to Do if You Want Duplicate MAC Addresses

You might want to duplicate MAC addresses. To configure ManageWise to allow duplicate MAC addresses, follow these steps:

Procedure
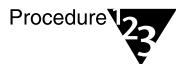
1. **Edit the NMS.INI file, which is in the Windows directory of the ManageWise Console, as follows:**

    1a. **Locate the [NETEXPLORER] section and find the last line that begins DupMac*n*=.**

    1b. **After that line, add a DupMac*n*=*MAC_address* line for each interface.**

    The value *n* is an ordinal number and *MAC_address* is the leading value of the special MAC address. In the DECnet example, *MAC_address* is AA-00-04.

    In writing the various instances of DupMac*n*, make sure you do not skip any numbers. If you skip any numbers, the values following the skipped number are not read. For example, if you skip from DupMac3 to DupMac5, the value of DupMac5, DupMac6, and all following numbers are not read.

The following is an example of a correctly configured NMS.INI file.

```
[NETEXPLORER]
;*****************************************
; NETEXPLORER-MANAGER TASK
;*****************************************
; A. NETEXPLORER MANAGER GLOBAL OPTIONS:
;------Do not change the following lines------
DllPath=C:\MW\NMS\BIN
DllFiles=n-snoopr,n-ipclnt,n_lsmmgr
AppType=background
AppTitle=NetExplorer Manager
AppIcon=C:\MW\NMS\BIN\NETXPLOR.ICO
DupMac1=AA0004
DupMac2=0000A2
DupMac3=000000
```

2. Close and save the NMS.INI file.

III Discovering Your Network

Discovery is the process by which ManageWise® software finds out the topology of your network so you can display, monitor, and manage your network from the ManageWise Console. Discovery involves two major parts of the ManageWise software:

◆ **NetExplorer**™ **software,** a set of NetWare® Loadable Module™ (NLM™) files that run on a ManageWise Server. (When NetExplorer is installed on a ManageWise Server, the server is called a NetExplorer Server.) NetExplorer discovers the network topology.

◆ **NetExplorer Manager,** a process that runs on the ManageWise Console. It reads the data discovered by NetExplorer and updates your ManageWise database to reflect changes to the network topology.

Chapter 4, "Network Discovery," describes the discovery processes and helps you fine-tune them so your database is kept up to date.

Chapter 5, "Troubleshooting Network Discovery," provides procedures for diagnosing difficulties with discovery, such as undiscovered devices or duplicate addresses.

chapter

4 *Network Discovery*

This chapter discusses using NetExplorer™ software and NetExplorer Manager to discover and maintain your network, especially after you complete the initial discovery cycle. For more information about the initial discovery cycle, refer to *ManageWise 2.6 Setup Guide.*

This chapter contains the following sections:

◆ "Understanding Discovery"

◆ "Monitoring and Configuring NetExplorer" on the ManageWise® Server

◆ "Scheduling and Running NetExplorer Manager" on the ManageWise Console

◆ "Maintaining the ManageWise Database" created by NetExplorer Manager

Understanding Discovery

This section provides a brief overview of the discovery process. When NetExplorer discovers your network, it gathers information about objects on your network and places them in the ManageWise database. This database is then used to create ManageWise maps that you can use to display your network's topology.

Understanding Discovery Cycles

NetExplorer Manager, running on the ManageWise Console, and NetExplorer, running on the NetExplorer Server, cooperate in discovering your network and updating the database that contains information about your network. NetExplorer on the NetExplorer Server automatically starts discovering your network topology when you start it for the first time. The information that NetExplorer

discovers is written to the SYS:\NMDISK\NETXPLOR.DAT file on the server.

NetExplorer Manager connects to the NetExplorer server. After the connection is established, NetExplorer on the server reads records from the SYS:\NMDISK\NETXPLOR.DAT file and sends them to NetExplorer Manager. NetExplorer Manager stores the records in a database.

Note ▼ If you stop NetExplorer Manager and start running it again later, NetExplorer Manager resumes receiving records from the point where it left off when you stopped.

Note ▼ Each NetExplorer Server supports up to five separate NetExplorer Manager connections at one time.

When you first start NetExplorer Manager, you should let it run as long as necessary to build the baseline data. How long this might take depends on the size of your network. Very small networks might take one or two hours; very large networks (several thousand nodes) might require a day or two.

Discovery starts when NetExplorer software is loaded on the NetExplorer Server. After NetExplorer is started, it runs as scheduled in NXPCON. (Refer to "Using NXPCON" on page 86.)

The discovery process occurs in cycles. A cycle is the process in which a discovery module identifies every node it can, one time. A cycle can be shortened or expanded by configuring NetExplorer on the server to discover certain addresses (refer to "Scheduling and Running NetExplorer Manager" on page 89).

The initial cycle continues until no additional devices are discovered. The amount of time required for this initial cycle depends on the size of the network.

Later cycles correct and complete the data gathered in earlier cycles. The initial cycle gathers information that might be insufficient to classify certain devices or to identify the correct segment for each device. But further discovery cycles provide additional, new, and changed information. The result is that as discovery cycles proceed, the information becomes more accurate.

Three independent discovery modules run in this order during each discovery cycle:

1. **IP discovery, on IP networks only.** This process, run by the NXPIP module, starts from the local router. Using the local router's routing table information, NXPIP discovers other routers on the network. It then uses the routing table information from each of the other routers to further discover the network. This process is repeated for each router discovered.

   If you are not running TCP/IP on your network, you need not run the NXPIP module.

2. **IPX™ discovery, on all networks, including NetWare®/IP™ networks.** This process, run by the NXPIPX module, starts at the NetExplorer Server itself to discover its IPX address, the LAN type of each adapter, and Service Advertising Protocol (SAP) information about other known devices and their services. After gathering this information, NXPIPX requests the same types of information from each device listed in the bindery (for NetWare 3.12 servers) or directory (for NetWare 4™ servers). This process is repeated each time NXPIPX discovers a new device.

Important ▼ You should always run IPX discovery as part of your discovery process, even if you have a NetWare/IP network.

Note ▼ A working directory, SYS:\NMDISK\NXPWORK, is created when NXPIPX.NLM is loaded. NXPIPX puts all its temporary files in this directory. Do not read, modify, or delete any file in this directory. Any of these actions might cause some discovery process to not function.

3. **Protocol-independent discovery by NetWare LANalyzer® Agent™ software.** This process, run by the NXPLANZ module, starts by identifying all the remote monitors (the NetWare LANalyzer Agent software and the LANtern™ network monitors). The NetWare LANalyzer Agent or LANtern network monitor on a segment discovers devices by the MAC address data contained in packets transmitted on the segment. The NXPLANZ module on the NetExplorer Server retrieves the data by using SNMP to communicate with NetWare LANalyzer Agent or LANtern network monitor.

   If you do not have NetWare LANalyzer Agent or LANtern network monitor installed, you need not run NXPLANZ.

During the initial discovery cycle, these modules run sequentially. As a result, information about NetWare LANalyzer Agent and LANtern network monitor is discovered late in the initial cycle.

In later discovery cycles, the three modules run concurrently. They continue their discovery processes but send only the new or changed data to NETXPLOR.NLM. As additional data arrives, segments can be consolidated, devices can be placed on the appropriate segments, and new devices can be discovered.

Each succeeding cycle has the potential to provide key items of information that finally identify a device and provide sufficient data for NetExplorer to consolidate the data provided by the different discovery NLM™ files.

Table 4-1 summarizes the default seed, default scope, required information, and user-definable information for each of the discovery modules. For information about setting the user-definable information using NXPCON, refer to "Monitoring NetExplorer" on page 87.

Table 4-1
Default, Required, and User-Definable Discovery Information

Discovery Module	Default Seed Information	Default Scope	User-Definable Changes
NXPIP	Examines the NetExplorer Server Routing table	Local IP network	Expand or reduce scope by specifying IP scope information in NXPCON
			If "public" SNMP community name is not used, list SNMP community names of routers in NXPCON
NXPIPX	Examines the NetExplorer Server's configuration	Entire IPX internetwork	Reduce scope by specifying IPX scope information in NXPCON
NXPLANZ	Examines the list of servers running NetWare LANalyzer Agent discovered by NXPIPX and LANtern network monitors listed in NXPCON	All segments with a NetWare LANalyzer Agent server or LANtern network monitor	Specify name and IP addresses of LANtern network monitors in NXPCON

Effects of Discovery on Maps

As information comes in to the database, ManageWise creates segments connected by routers on the internetwork map and displays objects on appropriate segment maps.

Most objects that ManageWise discovers are placed immediately on the correct segment. However, if too little information arrives to identify an object, it appears in a special segment called LOCATION UNKNOWN. This segment contains certain partially identified objects.

In some cases, devices are placed in the LOCATION UNKNOWN segment during the early discovery processes of the initial discovery cycle and are relocated to their correct segment when a later process provides additional information.

As described earlier, the IP discovery module (NXPIP.NLM) runs first if your network is running IP. The IPX discovery module (NXPIPX.NLM) runs second. The NetWare LANalyzer Agent discovery module (NXPLANZ.NLM) runs last. NXPLANZ.NLM can provide correct information for some of the devices placed in the LOCATION UNKNOWN segment.

Some specific devices and situations pose difficulties for NetExplorer. For example, some devices do not respond to IPX diagnostics packets, and some routing protocols require routers to duplicate the MAC address on all interfaces in each router. That leads to predictable NetExplorer difficulties that you might have to troubleshoot individually. For more information, refer to Chapter 5, "Troubleshooting Network Discovery."

Discovering NetWare SFT III Servers

A NetWare SFT III™ server usually consists of two computer systems, each containing an input/output engine (IOEngine) and a mirrored server engine (MSEngine). Therefore, physically there are two IOEngines and two MSEngines, logically there are two IOEngines and one MSEngine.

Note   An alternative to configuring two computer systems as an SFT III™ server is to configure a dual processor computer as an SFT III server.

The IOEngine is the part of the SFT III operating system that handles physical processes such as network and disk I/O, hardware interrupts, device drivers, timing, and routing. The MSEngine is the part of the SFT III server that handles nonphysical processes such as the NetWare file system, Novell® Directory Services™ (NDS™) software, and queue management.

NetExplorer fully discovers each IOEngine and puts it in the correct segment on the ManageWise maps. However, NetExplorer places the MSEngine in the LOCATION UNKNOWN segment. This happens because the two MSEngines are associated with only one logical server on the network, and the location of the MSEngine might change depending on which copy of the MSEngine is the primary at a given time. To move the MSEngine from the LOCATION UNKNOWN segment to the segment the server is actually on, follow the procedure in "Moving Nodes from Segment Map to Segment Map" on page 72.

If NetWare Management Agent™ is loaded on an SFT III server, the MSEngine and both of the IOEngines are discovered, as are their names.

If NetWare Management Agent is not loaded on the MSEngine, NetExplorer only discovers the MSEngine and the IOEngine that is the primary at the time of discovery. The primary IOEngine is labeled NONAME on the segment map. To change the name of an IOEngine on a segment map, follow the procedure in "Changing the Node or Segment Name" on page 57. To add the other IOEngine to the segment map, follow the procedures in "Adding a Node" on page 66.

Monitoring and Configuring NetExplorer

You use the NetExplorer Console, NXPCON, to configure and monitor NetExplorer on the NetExplorer Server. This section describes NetExplorer monitoring and configuration using NXPCON. It also tells you how to unload and reload NetExplorer at the NetExplorer Server. The final part of this section describes NetExplorer's behavior when you restart the NetExplorer Server.

Using NXPCON

NXPCON is loaded automatically when NetExplorer is loaded and is accessible at the NetExplorer Server or by selecting *Tools > Remote*

Console and opening a remote window to the NetExplorer Server within ManageWise.

If NXPCON is not loaded on your NetExplorer Server, check to see that NetExplorer is running. If NetExplorer is running, enter **LOAD NXPCON** at the system console prompt. If NetExplorer is not running, enter **NETXPLOR** at the system console prompt.

NXPCON contains context-sensitive help throughout. To access help in NXPCON, press F1.

Monitoring NetExplorer

The NXPCON main screen, shown in Figure 4-1, gives you information you can use to monitor the status of NetExplorer and of discovery.

Figure 4-1
NetExplorer Console Utility

◆ **NetExplorer Up Time**—Shows the time since NetExplorer started running.

- ◆ **Number of ManageWise Consoles Attached**—Shows the number of ManageWise clients that are currently attached and receiving discovered information from this server. You can have up to five consoles attached simultaneously to one NetExplorer Server.

- ◆ **NetExplorer System Status**—Shows the overall status. It can have one of two values:

  - ◆ **Initial cycle in progress**—One or more of the discovery modules (NXPIP, NXPIPX, or NXPLANZ) has not yet completed its first cycle.

  - ◆ **Initial cycle complete**—All modules have completed at least one pass.

- ◆ **Module Status**—Shows the status of each module and the number of cycles that module has completed. For example, in Figure 4-1, NXPIP is not loaded, while NXPIPX and NXPLANZ are running. The module status can be one of the following values:

  - ◆ **Not Loaded**—Module is not loaded.

  - ◆ **Waiting to Start**—Module is loaded but not started.

  - ◆ **Running**—Module is running and collecting data.

  - ◆ **Suspended**—Module is suspended because the end of the schedule in which it was running was reached.

  - ◆ **Completed**—Module completed a discovery cycle.

  - ◆ **Unknown**—NetExplorer cannot obtain the module status. (This is usually seen if the module is not loaded.)

Unloading and Reloading NetExplorer

To unload and reload NetExplorer, follow these steps:

Procedure
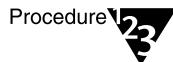
1. At the NetExplorer Server, unload the NetExplorer NLM files by entering the following command at the server prompt:

UNXP

This command unloads the NetExplorer modules in the correct order.

2. Load the NetExplorer modules again by entering the following command at the server prompt:

`NETXPLOR`

This command loads the NetExplorer modules in the correct order.

Note ▼ Each time you reload the NetExplorer modules, a new version of NETXPLOR.DAT is created. Information from a previous run of the NetExplorer modules is lost.

Restarting the NetExplorer Server

If you bring down the NetExplorer Server, for example, for maintenance, the restart affects NetExplorer in the following ways:

1. All previously discovered information is lost from the server memory (NETXPLOR.DAT). The ManageWise database on the ManageWise Console remains intact, however.

2. The initial discovery cycle starts again.

3. NetExplorer Manager processes all the discovery data again as NetExplorer rediscovers the network.

4. NetExplorer Manager compares the new data with the contents of the database, retaining new information and discarding all the duplicated information, and updates the database.

Bringing down the NetExplorer Server has no other effect on the database because the database is maintained by the ManageWise Console, not by the NetExplorer Server.

Scheduling and Running NetExplorer Manager

NetExplorer Manager is the ManageWise Console software that controls when data is retrieved from NetExplorer on the server and when the ManageWise database is updated. You can make the following decisions about running NetExplorer Manager:

◆ When to start NetExplorer Manager the first time

◆ How to schedule updates

◆ Whether to close NetExplorer if it is running in the background when ManageWise is running

This section provides tips that tell you how you can make these decisions.

Running NetExplorer Manager

Depending on the size of your network, writing data from the initial discovery cycle can take a few minutes or as long as several days. Subsequent discovery updates to the ManageWise database require substantially less time.

Note   During initial discovery, database writing activities can tie up your ManageWise Console, slowing its performance.

After the initial discovery, you can stop the NetExplorer Manager software on the ManageWise Console or let it run in the background. Even if you close NetExplorer Manager on the ManageWise Console, you should run it periodically to update the database.

NetExplorer continues to run on the NetExplorer Server as scheduled, even if you stop NetExplorer Manager updates on the ManageWise Console.

After the initial discovery is complete, you might want to schedule NetExplorer Manager to run periodically rather than continually. By running NetExplorer Manager periodically, you can update the database at times that do not interfere with other management activities.

Scheduling NetExplorer Manager Updates

After initial network discovery is completed and the baseline data is sent to the ManageWise Console, you can set a schedule for further NetExplorer Manager update operations. You can configure NetExplorer Manager to run continually or periodically at the same time every day, or you can start it manually whenever you want. (For example, you can schedule NetExplorer Manager to run every day for 8 hours, starting at 10 p.m.) The default configuration is to let it run continually.

NetExplorer Manager runs as scheduled, provided that your PC is turned on and Windows is running.

Depending on how you schedule, NetExplorer Manager runs as follows:

◆ If you configure NetExplorer Manager to run continually, it starts each time you start Windows.

◆ If you want to run NetExplorer Manager daily, you can specify a specific time and duration. NetExplorer Manager runs at that time *if Windows is running*. If Windows is not running, NetExplorer Manager does not run either.

◆ If you set NetExplorer Manager to run only on demand, you must double-click the NetExplorer Manager icon in the ManageWise program group to start it.

Note NetExplorer Manager scheduling does not need to be synchronized with NetExplorer scheduling. To add the most complete information to the database, schedule NetExplorer Manager to run after NetExplorer finishes running. For information about scheduling NetExplorer, refer to *ManageWise 2.6 Setup Guide.*

Starting NetExplorer Manager Manually

If you want to start NetExplorer Manager at an unscheduled time, double-click the NetExplorer Manager icon in the ManageWise program group. NetExplorer Manager begins to communicate with NetExplorer and to update information in the database, as needed. If your network has changed very little since the previous update, it might take only a few seconds to complete.

Viewing the Status of NetExplorer Manager

You can view NetExplorer Manager status when it is running by clicking the NetExplorer Manager icon and selecting *About NetExplorer Manager*. The NetExplorer Manager dialog box appears. This dialog box lists the name of the server to which NetExplorer is connected, whether NetExplorer is currently connected to that server, and the number of records NetExplorer Manager received from that server.

Note ▼ ManageWise suspends NetExplorer Manager operation while it displays the NetExplorer Manager dialog box.

Maintaining the ManageWise Database

Maintaining the ManageWise database is relatively simple. The ManageWise database resides on the ManageWise Console. To maintain the database, you need to run NetExplorer Manager at intervals so changes in network topology are reflected in the data. You also need to delete saved alarms from the database periodically to prevent the alarm log files from filling your hard disk. You can use the ManageWise Database Administration Tool to complete these tasks.

Database Administration Tool

The Database Administration Tool lets you back up, restore, and reset the ManageWise database. It also lets you delete saved alarms, reset traps, and reset the network topology. For information about deleting saved alarms and resetting traps, refer to "Deleting Selected Alarms" on page 147 and "Resetting Traps" on page 325, respectively.

Starting the Database Administration Tool

To start the Database Administration Tool, follow these steps:

Procedure ▼
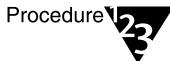
1. **Close all ManageWise applications.**

   When the Database Administration Tool is started, it tries to shut down any ManageWise application that is running. If the application cannot be shut down, the Database Administration Tool prompts you that it cannot continue and exits.

2. **Double-click the Database Administration Tool icon in the ManageWise program group.**

   You are prompted to enter a password.

3. **Enter your ManageWise Console password.**

   The system displays the ManageWise Database Administration dialog box.

4. **To select an option, click it.**

To get help at any time, click the Help button or press F1.

Database Maintenance Tasks

You should back up your database before using any of the other Database Administration Tool options. The sections that follow explain other database maintenance tasks in detail.

Handling a Power Failure or a Software Problem

The Btrieve* record management system has a mechanism that prevents a power failure or software problem from corrupting the ManageWise database during modifications. When ManageWise first writes to the database in any session, the Btrieve record management system creates a pre-image file. If the power is disrupted or a software problem causes the system to crash, Btrieve uses the information in the pre-image file to restore the database to its previous state.

The Btrieve pre-image file has the extension .PRE and is stored in the \MW\NMS\NMSDB directory with the other database files.

Warning　You should *never* erase, move, or otherwise disturb a .PRE file. Without it, Btrieve cannot recover from a power failure or software problem.

Backing Up Disk Files

To protect yourself from potential hard disk problems, you must back up files frequently. The Btrieve record management system .PRE files do not protect you from a hardware problem or hard disk failure.

Restoring an Old Database

You might need to restore a copy of a database that was backed up previously. You might need to do so if, for example, your database files got corrupted or if you selected a Database Administration Tool option and did not like the results.

Resetting Network Topology

Resetting the network topology does the following to the ManageWise database and internetwork map:

◆ Deletes all segments in the ManageWise database except the LOCATION UNKNOWN segment. This includes any segment you added manually by selecting *Edit > Add* (refer to "Adding Objects to Maps and to the Database" on page 64).

◆ Moves all the nodes that were on the deleted segments to the LOCATION UNKNOWN segment. This includes all nodes you added manually by selecting *Edit > Add.* Services that you added to nodes or equipment and contact information about nodes are not removed.

◆ Logically connects all network adapters to the LOCATION UNKNOWN segment. Other network adapter information is not changed.

To correct the ManageWise database and rebuild ManageWise maps, you can either rediscover the internetwork using NetExplorer or re-create the internetwork manually by selecting *Edit > Add.* The following occurs if you rediscover the internetwork using NetExplorer:

◆ Any nodes not discovered by NetExplorer remain in the LOCATION UNKNOWN segment.

◆ Nodes that you added manually by selecting *Edit > Add* and that NetExplorer discovered remain in the LOCATION UNKNOWN segment only if you selected the Prevent Deletion By NetExplorer check box when adding the node.

◆ Network adapter information, saved when you reset network topology, might change.

You might need to reset the network topology in the following cases:

◆ If ManageWise has overconsolidated your segments. This means that ManageWise considers two or more segments to be on the same physical cable, when in reality they are not. In this case, you need to reset the network topology and consolidate the segments manually. If you do not consolidate the segments, a device might first appear on one segment and then on the other without your knowing where to find the device or even that it is the same single device.

◆ If you have made significant changes to your physical network topology. Using this option forces ManageWise to rediscover the

network topology. For this to be most effective, you must unload the NetExplorer NLM files from the NetExplorer Server and then reload them after you have reset the network topology.

Note ▼ Because of the amount of time involved in resetting topology, we recommend that you select segments that you do not want on the internetwork map and delete them. Reset the topology or the database as a last resort.

Correcting Overconsolidated Segments

If ManageWise has overconsolidated your segments, follow these steps:

Procedure ▼ **1. Start the Database Administration Tool as explained in "Starting the Database Administration Tool" on page 92.**

2. Back up your existing database by selecting the Back Up Current Database option.

3. Reset the network topology by selecting the Reset Network Topology option.

When you select this option, the system calculates and displays the amount of time the reset will take. If you do not want to continue with the reset, you can cancel it now or at any time during the reset.

Important ▼ If you cancel the request after the reset has started, it might mean that only part of the topology has been reset or only part of the network has been reset. If you cancel the request after a segment is partially reset, the Database Administration Tool continues the process until the whole segment is reset. If your network has been only partially reset, you must run NetExplorer Manager again to rediscover the reset segments and networks.

While topology is being reset, your system is still usable. However, you cannot run any ManageWise applications.

4. Exit the Database Administration Tool and start ManageWise.

5. Disable segment consolidation.

To do so, select *Configure > Global Preferences > NetExplorer Options* and deselect the Consolidate IP-IPX Segments check box.

6. Run NetExplorer Manager again by double-clicking the NetExplorer icon in the ManageWise program group.

Your system remains accessible while NetExplorer Manager is running. However, NetExplorer Manager stops whenever you access your system, slowing down the addition of data to the database. Therefore, you might want to run it overnight or over a weekend.

7. **Manually consolidate the selected IP and IPX segments that you want consolidated.**

Correcting Network Topology

If you have made significant changes to your physical network topology, unload the NetExplorer NLM files from the NetExplorer Server and then reload them after you have reset the network topology. To do so, follow these steps:

Procedure

1. **On the NetExplorer Server, unload the NetExplorer NLM files by entering the following command at the server prompt:**

   UNXP

2. **Shut down the ManageWise Console and close all ManageWise applications.**

3. **Start the Database Administration Tool as explained in "Starting the Database Administration Tool" on page 92.**

4. **Back up your existing database by selecting the Back Up Current Database option.**

5. **Reset the network topology by selecting the Reset Network Topology option.**

   Resetting the network topology could take a long time for large networks. Refer to Step 3 of the "Correcting Overconsolidated Segments" procedural steps for an explanation of this option.

6. **Reload the NetExplorer NLM files on a NetExplorer Server by entering the following command at the server prompt:**

   NETXPLOR

7. **At the ManageWise Console, run NetExplorer Manager by double-clicking the NetExplorer icon in the ManageWise program group.**

Your system remains accessible while NetExplorer Manager is running. However, NetExplorer Manager stops whenever you access your system, slowing down the addition of data to the database. Therefore, you might want to run it overnight or over a weekend.

Resetting the Database

Reset the ManageWise database if you want to empty it. Resetting the database deletes all objects from it, including all saved alarms, the ManageWise Console password, and all user-entered configuration and locational information.

We recommend that before selecting this option, you back up your existing database using the Back Up Current Database option. After you reset your database, you must run NetExplorer Manager again. To reset the database, follow these steps:

Important ▼ Use this option *only* if you want to delete all information in the database, including information you have entered.
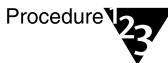
Procedure ▼ 1. **Start the Database Administration Tool as described in "Starting the Database Administration Tool" on page 92.**

2. **Back up your existing database by selecting the Back Up Current Database option.**

3. **Reset the database by selecting the Reset Database option.**

4. **Reinstall any third-party software.**

5. **Recompile MIBs by selecting *Tools > SNMP MIB Compiler*.**

6. **Run NetExplorer Manager by double-clicking the NetExplorer icon in the ManageWise program group.**

Your system remains accessible while NetExplorer Manager is running. However, NetExplorer Manager stops whenever you access your system, slowing down the addition of data to the database. Therefore, you might want to run it overnight or over a weekend.

chapter **5** *Troubleshooting Network Discovery*

Sometimes, because of the peculiarities of certain types of systems, NetExplorer™ software discovers incomplete or conflicting information. This might result in maps that do not look accurate and system information that is incomplete. This chapter describes various actions you can take to correct for such systems, in the following categories:

◆ Difficulties with basic discovery, such as systems not being discovered or not responding to NetExplorer. Refer to "Correcting Difficulties with Basic Discovery."

◆ Problems with scoping discovery, such as your database containing nodes outside the scope you set or not containing nodes within scope. Refer to "Correcting Problems with Discovery Scope" on page 108.

◆ Moving nodes from the LOCATION UNKNOWN segment. Refer to "Moving Nodes from the LOCATION UNKNOWN Segment" on page 113.

◆ Correcting duplicate, wrong, or multiple addresses. Refer to "Correcting Duplicate, Wrong, or Multiple Addresses" on page 115.

◆ Correcting the display of bridges and routers on the maps. Refer to "Correcting Difficulties with Bridges and Routers" on page 122.

The final section of the chapter describes how to create a NETXPLOR.DAT backup file if you need it for troubleshooting and technical support purposes.

Correcting Difficulties with Basic Discovery

Typical errors you can easily correct include the following:

◆ New or existing nodes, including LANtern™ network monitors or servers running NetWare® LANalyzer® Agent™ software, that are not discovered

◆ Servers that are discovered but not named on the map

◆ Overconsolidated segments

◆ Servers that are not responding to NetExplorer

◆ Nodes no longer on your network

◆ Wrong icons used for a node

◆ Names of discovered systems are not descriptive

◆ Duplicate nodes with different MAC addresses

Nodes Not Discovered

Sometimes new or existing systems are not discovered because NetExplorer has not discovered the node yet or because NetExplorer cannot access the system. The following sections describe solutions to these difficulties:

◆ New Node Not Discovered

◆ Existing Node Not Discovered

New Node Not Discovered

If you have recently added a new node to your network but NetExplorer has not discovered it yet, you can add it to the map manually. NetExplorer then updates information about the node when the node is discovered.

Refer to "Adding a Node" on page 66 for information about adding a node to the map.

If you have just installed a new NetWare LANalyzer Agent server and want NetExplorer to query it immediately, add it to the list of NetWare LANalyzer Agent servers in NXPCON, then restart NetExplorer on the NetExplorer Server. Refer to "NetWare LANalyzer Agent Servers Not Discovered" on page 102.

Existing Node Not Discovered

If you have an existing node that is not being discovered, check the following:

◆ SNMP community names in NXPCON. The node might have a community name assigned that is not in the list of acceptable SNMP community names. To correct this, refer to "Adding an SNMP Community Name."

◆ NetExplorer Server configuration. Refer to "Checking NetExplorer Server Configuration" on page 102.

◆ Whether the node is a LANtern network monitor or NetWare LANalyzer Agent on an IP-only segment. Refer to "NetWare LANalyzer Agent Servers Not Discovered" on page 102.

Adding an SNMP Community Name

To add an SNMP community name, follow these steps:

Procedure 23
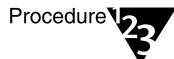
1. **Find out the SNMP community name assigned to the undiscovered system.**

2. **In the ManageWise® program, select *Tools > Remote Console* to open a remote console window on the NetExplorer Server.**

   Work at the NetExplorer Server console directly.

3. **Go to the NXPCON screen.**

   If NXPCON is not loaded, enter **LOAD NXPCON** at the system prompt.

4. **In the Configuration Options window, use the arrow keys to move the highlight bar to *SNMP*, and then press** Enter**.**

   NXPCON displays the list of SNMP configuration options.

5. **Select** *Edit Community Name List*, **and then press** Enter.

   NXPCON displays the community names.

6. **Press** Insert.

   NXPCON displays a box in which you can enter the new name.

7. **Enter the community name for the undiscovered system.**

   NXPCON displays the list, which now includes the new name.

8. **Repeat Step 6 and Step 7 for each name you need to add.**

9. **Press** Esc **twice to close the list and the SNMP window.**

10. **Select** *Activate Changes*, **and then press** Enter.

    NXPCON activates your changes.

    NetExplorer can now query the node the next time it runs. You might want to select *Discovery Schedule* and modify the discovery schedule, if necessary, to cause NetExplorer to run sooner.

Checking NetExplorer Server Configuration

Sometimes, when the NetExplorer Server does not discover systems, the cause is the configuration of the server itself. For example, a common problem is for the NetExplorer Server's internal network address to be the duplicate of a physical address elsewhere on the network. In this case, the system with the same address is not discovered, or is discovered inaccurately. Change the internal address of the NetExplorer Server to solve this problem.

NetWare LANalyzer Agent Servers Not Discovered

NetExplorer automatically discovers NetWare LANalyzer Agent servers on IPX™ segments. However, if you have NetWare LANalyzer Agent servers on IP-only segments, you must add them to the list in the NetExplorer Console (NXPCON) before NetExplorer queries them.

To add a NetWare LANalyzer Agent server or LANtern monitor in NXPCON, follow these steps:

1. **In ManageWise, select *Tools > Remote Console* to open a remote console window on the NetExplorer Server.**

   Or, work at the NetExplorer Server console directly.

2. **Go to the NXPCON screen.**

   If NXPCON is not loaded, enter `LOAD NXPCON` at the system prompt.

3. **In the Configuration Options window, use the arrow keys to move the highlight bar to *NXPLANZ Discovery*, and then press** Enter**.**

   NXPCON displays the list of NetWare LANalyzer Agent servers and LANtern monitors.

4. **Press** Insert **to add a NetWare LANalyzer Agent server to the list.**

5. **Enter the name and address of the agent. Select the correct agent type.**

6. **Press** Esc**, and then select Yes to save your changes.**

   NXPCON displays the NetWare LANalyzer Agent window and adds the agent to the list.

7. **Repeat Step 4 through Step 6 for each agent you need to add.**

8. **When you are finished, press** Esc **to close the list.**

9. **If you have made changes to options other than *NXPLANZ Discovery*, select *Activate Changes*, and then press** Enter**.**

   NXPCON warns you that you must restart NetExplorer for the change to the NetWare LANalyzer Agent list to take effect. However, other changes you have made in NXPCON are activated at this time.

10. **At the system console prompt, unload and reload NetExplorer (refer to "Unloading and Reloading NetExplorer" on page 88).**

NetExplorer queries the newly listed agents the next time it runs the NXPLANZ discovery module. You might want to check the discovery schedule and modify it, if necessary, to cause NetExplorer to run sooner.

Note ▼   Restarting NetExplorer on the server does not reset the database on the ManageWise Console. NetExplorer Manager updates the database the next time it runs.

Workstation Name Not Discovered

If NetExplorer cannot find the client workstation name, the MAC address of the workstation is used. Client workstation names are retrieved from servers running NetWare Management Agent. Refer to *ManageWise 2.6 Setup Guide* for an explanation of how ManageWise displays the names of discovered objects.

You can add the workstation name to the database manually by selecting *Edit > Database Object*. For more information about this command, refer to "Changing the Node or Segment Name" on page 57.

Server Name Not Discovered

If a server is discovered but its name is not shown on the map, the server is probably in scope for IP discovery but out of scope for IPX discovery. Scoping for the two protocols can be set differently. NXPIP can discover a server if it is routing, but NXPIPX, the IPX discovery module, is responsible for discovering server names.

You can repair this problem in one of two ways:

◆ Correct the IPX scope to include the server. Refer to "Changing the Scope of Discovery" on page 109.

◆ Add the server name to the database manually by selecting *Edit > Database Object*. For more information about this command, refer to "Changing the Node or Segment Name" on page 57.

Overconsolidated Segments

On routers with NetWare MultiProtocol Router™ software and multiple-port WAN interfaces connected to different networks, ManageWise discovers the interfaces but does not discover the ports.

The IPX networks connected to the ports on a single interface are consolidated as a single network.

If your network segments are overconsolidated, follow these steps:

1. **Edit the NMS.INI file, which is located in the Windows directory of the ManageWise Console, as follows:**

   1a. **Locate the [NETEXPLORER] section and find the last line that begins DupMac*n*=.**

   1b. **After that line, add a DupMac*n*=*MAC_address* line for each interface.**

      Where *MAC_address* is the MAC address of one of the WAN interfaces in the router.

      In writing the various instances of DupMac*n*, make sure you do not skip any numbers. If you skip any numbers, the values following the skipped number are not read.

      For example, if you skip from DupMac3 to DupMac5, the value of DupMac5, DupMac6, and all following numbers is not read. The following is an example of a correctly configured NMS.INI file.

```
[NETEXPLORER]
;**********************************************
;                      NETEXPLORER-MANAGER TASK
;**********************************************
; A. NETEXPLORER MANAGER GLOBAL OPTIONS:
;------Do not change the following lines------
DllPath=C:\MW\NMS\BIN
DllFiles=n-snoopr,n-ipclnt,n_lsmmgr
AppType=background
AppTitle=NetExplorer Manager
AppIcon=C:\MW\NMS\BIN\NETXPLOR.ICO
DupMac1=AA0004
DupMac2=0000A2
DupMac3=000000
```

2. **Delete the overconsolidated segment from the internetwork map.**

   Deleting the overconsolidated segment from the internetwork map also deletes the segment from any other maps and from the

database. To delete the segment from the internetwork map, follow these steps:

2a. Click the overconsolidated segment.

2b. Press Del**.**

3. At the system console prompt, unload and reload NetExplorer.

Refer to "Unloading and Reloading NetExplorer" on page 88.

After reloading NetExplorer on the server, run NetExplorer Manager (double-click the NetExplorer Manager icon in the ManageWise program group) to add new data to the database.

Servers Not Responding to NetExplorer

Sometimes improperly configured NetWare LANalyzer Agent servers do not respond or cease to respond to requests for real-time information about the segment. Sometimes NXPIP cannot communicate with an IP router. The cause typically centers around incorrect SNMP command-line parameters or community names.

NetWare LANalyzer Agent Does Not Respond

If NetWare LANalyzer Agent does not respond, SNMP might have been loaded with incorrect command-line parameters.

To correct this problem, follow these steps:

Procedure
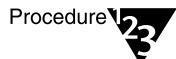
1. Open the AUTOEXEC.NCF file on the NetWare LANalyzer Agent server.

2. Edit the line that loads SNMP to match the following:

```
LOAD SYS:\SYSTEM\SNMP CONTROL= TRAP=
```

SNMP must be loaded with the parameters shown.

If SNMP.NLM is already loaded, you can add the CONTROL and TRAP parameters by entering the following:

```
SNMP CONTROL= TRAP=
```

IP Router Does Not Respond

If an IP router does not respond, its SNMP community name might have been set to something other than *public*, the default name used by ManageWise.

To correct this problem, add the router's community name to NetExplorer's list of community names. To add the router's community name, follow the steps shown for "Adding an SNMP Community Name" on page 101.

Nodes No Longer on Your Network

Systems that you removed from the network still appear in ManageWise maps. NetExplorer does not remove nodes that are no longer on the network from the database. To remove a node from ManageWise maps and from the database, follow the procedure listed in "Deleting Objects" on page 71.

Wrong Icons Used for a Node

Occasionally, the wrong icon is used for a node. An example is source-route bridged token rings. The bridge is discovered but is not shown on ManageWise maps as a bridge. Instead, each interface of the bridge is shown as a separate node.

To change the icon, follow the steps shown for "Changing the Node Icon" on page 53.

Names of Discovered System Are Not Descriptive

Systems without associated names are identified on ManageWise maps using addresses. Addresses might not be descriptive enough to identify systems immediately. To change the name of a discovered system, follow the steps shown for "Changing the Node or Segment Name" on page 57.

Duplicate Nodes with Different MAC Addresses

If you replace an Ethernet card on your system, NetExplorer discovers the system again with the same IP address, network services, and server

name, but with the new MAC address. This results in two nodes on ManageWise maps with the same node information but with different MAC addresses.

To delete the node represented by the replaced Ethernet card from the database and maps, follow the steps shown for "Deleting Objects" on page 71.

Correcting Problems with Discovery Scope

Common problems with discovery scope include the following:

◆ Some of your network is not being discovered.

◆ NetExplorer is querying systems it should not.

◆ NetExplorer is discovering segments that you do not want on your maps.

◆ You have done a topology reset, but nodes you thought would be deleted by the reset are still on your maps (in the LOCATION UNKNOWN segment).

The following sections discuss ways of fixing these difficulties.

Parts of the Network Not Discovered

If your database does not reflect all your network, there are several possible causes:

◆ NetExplorer Manager on the ManageWise Console has not finished reading all the data from NetExplorer. Leave NetExplorer Manager running overnight or over a weekend and see whether the problem corrects itself.

◆ Your discovery scope settings in NXPCON are too restrictive. You might want to adjust the scope in increments, as described in "Adjusting Scope Incrementally" on page 110.

◆ If a particular segment that you know is in the defined scope is not being discovered, your discovery scope might not be defined as a

contiguous area. Refer to "Adjusting Scope Incrementally" on page 110.

Changing the Scope of Discovery

To change the scope of IP or IPX discovery, follow these steps:

Procedure

1. **In ManageWise, select *Tools > Remote Console* to open a remote console window on the NetExplorer Server.**

   Or, work at the NetExplorer Server console directly.

2. **Go to the NXPCON screen.**

   If NXPCON is not loaded, enter **LOAD NXPCON** at the system prompt.

3. **In the Configuration Options window, use the arrow keys to move the highlight bar to *Discovery Scope*, and then press** Enter**.**

4. **Select either *IP Discovery Scope* or *IPX Discovery Scope*, and then press** Enter**.**

5. **You can either edit your existing scope or add a new, contiguous set of network addresses to the scope.**

Note

A contiguous set of network addresses is a collection of interconnected network segments, all of which are defined in the scope. An example of segments that are not contiguous is shown in "Adjusting Scope to Be Contiguous" on page 111.

   ◆ To edit an existing scope constraint, select it, and then press Enter.

   ◆ To add a new entry, press Insert.

6. **Enter the network address (for IP) and the mask, or enter the network number (for IPX) and the mask.**

   Press F1 for help on defining a mask.

7. **Press** Esc **and select Yes to save your changes.**

   NXPCON displays your changes in the IP or IPX Discovery Scope list.

8. **Repeat Step 5 through Step 7 for each additional entry.**

9. **Press** Esc **twice to close the Discovery Scope windows.**

10. **If you have made changes to options other than scope, select** *Activate Changes***, and then press** Enter**.**

    NXPCON warns you that you must restart NetExplorer for the change in scope to take effect. However, other changes you have made in NXPCON are activated at this time.

    Important

    If you are correcting a database scope that is too large, as described in "NetExplorer Discovering Too Much" on page 112, stop here and return to that procedure.

11. **At the system console prompt, unload and reload NetExplorer.**

    Refer to "Unloading and Reloading NetExplorer" on page 88. NetExplorer now discovers nodes in the new scope you defined.

Adjusting Scope Incrementally

You might want to adjust the scope in small increments, adding a segment or two at a time and allowing NetExplorer to discover the additional segments before adding more. You should do this for IPX networks whose addresses were assigned randomly. For such networks, it is difficult to define a scope that includes the entire network.

For example, you could begin with a scope that includes only the segment the NetExplorer Server is on. NetExplorer discovers that segment, all routers attached to it, and all segments immediately on the other side of the routers. NetExplorer does not discover nodes beyond the scope you defined. For example, it does not discover any nodes on the segments on the far side of the routers.

Note

The segment icon for the segments discovered outside of the scope appear on the internetwork map. These segments contain one node: the router connected to a node within the defined scope. This is the way scoping works. Trying to delete the segments to simplify the map only works temporarily. The next time NetExplorer runs, it adds back the segments to the database and maps.

Now you have the addresses of the segments on the far side of the routers, shown on the internetwork map, and can add them to your discovery scope in NetExplorer. NetExplorer adds nodes on these

segments, including routers, and discovers the segments immediately on the other side of the new routers.

You can continue adding segments incrementally until NetExplorer has either discovered the portion of the network of which you are interested or discovered your entire network.

Adjusting Scope to Be Contiguous

If you have defined a discovery scope for IP or IPX that includes a particular segment and that segment is not being discovered, make sure the scope you have defined is contiguous.

For example, suppose you have three segments, A, B, and C, and segment B connects A and C (refer to Figure 5-1). You define a scope that includes A and C but not B. In this case, only segment A is discovered. Segment C is not discovered because NetExplorer stops at segment B, which is not in the scope.

Figure 5-1
Contiguous Scoping Example
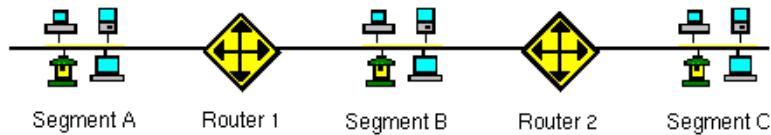
To correct this problem, change the scope definition to include segment B. NetExplorer can then discover segments B and C as well as segment A.

NetExplorer Querying Systems It Should Not

Occasionally, NetExplorer queries a system that is configured to notify its user if queried by SNMP. If you have systems on your network that you do not want to query, use the SNMP exclusion option in NXPCON (refer to "Using NXPCON" on page 86).

NetExplorer Discovering Too Much

If NetExplorer discovers segments that you do not want on your maps, you need to make your discovery scope smaller.

Note ▼ NetExplorer always discovers the existence of segments on the far side of routers at the scope boundary. These segments are saved in the database and shown on the internetwork map. Nodes for these segments are not in the database and are not shown on the internetwork map because these segments are outside of the discovery scope.

To make your discovery scope smaller, follow these steps:

Procedure ▼
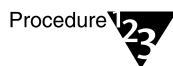
1. **Close NetExplorer Manager at the ManageWise Console.**

2. **In NXPCON on the NetExplorer Server, change the scope of discovery to reflect the smaller scope.**

   Refer to "Changing the Scope of Discovery" on page 109. However, *do not restart NetExplorer on the server yet.*

3. **Delete any unwanted segments from the internetwork map by selecting the segment and pressing** Delete**.**

   You can delete a number of segments at one time by holding down Ctrl while selecting unwanted segments, then pressing Delete.

Note ▼ Deleting the segment from a map also deletes the segment from the database.

Important ▼ Alternatively, at the ManageWise Console, use the Database Administration Tool to back up and reset the database.

Resetting the database deletes *all* your changes, including custom maps, added objects, and changes you have made with the Database Object Editor. You must reenter these changes after the reset. You should consider whether deleting objects would be more time-consuming than reentering changes after resetting the database.

4. **After you complete your changes to the database, unload NetExplorer (using the UNXP command at the server console prompt) and reload it (using the NETXPLOR command).**

   Restarting NetExplorer deletes the NetExplorer records on the server. Because NetExplorer must start from scratch in discovering your network, only objects within the new scope you defined are discovered.

5. After restarting NetExplorer, run NetExplorer Manager at the ManageWise Console.

NetExplorer Manager reads the new discovery data from the server, re-creating a database with the new, smaller scope.

After Topology Reset, Extraneous Systems Are Still on the Map

Resetting the network topology removes network connection information but does not remove systems from the database. As a consequence, systems that were once discovered but either no longer exist or have been removed from your monitored networks might still appear in the LOCATION UNKNOWN segment.

Note ▼▲ Topology Reset is only recommended when you make major changes to your topology. Major changes require the complete rediscovery of the network topology by NetExplorer.

To delete those systems from the database, follow these steps:
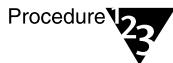
Procedure ▼23▲
1. Select the system in the LOCATION UNKNOWN segment.

2. Select *Edit > Delete*.

3. Click Yes when a message box prompts you to remove the system from the database and maps.

The system icon is then removed from the LOCATION UNKNOWN segment and from the ManageWise database.

For more information about resetting the network topology and other uses of the Database Administration Tool, refer to "Resetting Network Topology" on page 93.

Moving Nodes from the LOCATION UNKNOWN Segment

Some systems might be in the LOCATION UNKNOWN segment because they do not respond to IPX diagnostic requests or they no longer exist. Systems that exist but do not respond can be moved from the LOCATION UNKNOWN segment in one of the following ways:

◆ Automatically by NetExplorer Manager (refer to "Systems That Are Automatically Relocated")

◆ Manually (refer to "Moving Systems to the Correct Segment")

Systems That Are Automatically Relocated

NetExplorer Manager periodically examines the LOCATION UNKNOWN segment for any system with an IPX address that corresponds to an associated IPX network on ManageWise maps. If NetExplorer Manager finds such a system, it automatically relocates the system to the known IPX network.

If the first 4 bytes of the address do not correspond to a known IPX network, the system cannot be relocated; it remains in the LOCATION UNKNOWN segment.

Moving Systems to the Correct Segment

The following systems are initially placed in the LOCATION UNKNOWN segment when discovered by NetExplorer:

◆ NetWare for UNIX servers

◆ Access servers

◆ Modem servers

◆ Print servers

◆ NetWare SFT III™ MSEngines

You can move these systems to the correct segment by configuring them with the appropriate network address information.

To configure the systems (thus removing them from the LOCATION UNKNOWN segment), follow these steps:

Procedure

1. **Open the LOCATION UNKNOWN segment.**

   Select *View > Find > Segment* to find the LOCATION UNKNOWN segment on your internetwork map.

2. **Click a system to select it.**

3. **Select *Edit > Database Object*.**

4. **Scroll down to the Adapter Information icon and click it.**

5. **Click Edit.**

6. **Enter the correct information for the MAC address and IP or IPX address of the system.**

7. **Select the correct network segment (IP or IPX) from the drop-down list.**

8. **Enter information about the make and model if the field is blank.**

   This is optional information.

9. **Click OK.**

   The new information is entered in the database and the system is moved to the segment you specified on the internetwork map.

10. **Close the dialog box.**

Correcting Duplicate, Wrong, or Multiple Addresses

Sometimes NetExplorer cannot discover correct addresses for a system. This section explains how to correct multiple segment addresses, unknown MAC addresses, and non-unique MAC addresses.

NetExplorer Displaying Multiple Network Addresses for Segment

Segments are rarely displayed with multiple IP addresses or multiple IPX addresses or both.

Multiple IP addresses are shown only if you have multiple IP networks on the same segment cable. This does not indicate a ManageWise discovery error.

Multiple IPX addresses can be shown if a router connected to the segment is misconfigured to have IPX network addresses it should not have. To fix this problem, change the router configuration to indicate the correct network bound to the adapter.

Note ▼ There are configurations in which multiple IPX address are valid. For example, multiple IPX addresses can occur if there are two different frame types running with different IPX network numbers.

Nodes with Unknown MAC Addresses

ManageWise gives the MAC address 00-00-00-00-00-00 to nodes whose MAC address it cannot identify. If you want to update a MAC address, follow these steps:

Procedure ▼ 23
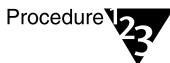
1. **In ManageWise, select the node on a map.**

2. **Select *Edit > Database Object* or click the Edit Object button on the action bar.**

   ManageWise displays the Database Object Editor.

3. **Select *Adapter Information*.**

   ManageWise displays the adapter information and details for the object.

4. **Click the Edit button.**

   ManageWise displays the Edit Network Interface dialog box.

5. **Enter the address information, then click OK.**

   ManageWise updates the MAC address.

6. **Close the dialog box.**

Nodes without Unique MAC Addresses

Some nodes with multiple network interfaces do not assign an individual MAC address to each interface. For example, Bay Networks, DECnet*, and XNS* routers fall into this category. When interfaces do not have individual MAC addresses, ManageWise discovery modules get confused, and you might have to take some corrective action at the end of the initial discovery cycle.

Depending on the network protocols in use and the ManageWise discovery modules that are loaded (NXPIP, NXPIPX, and NXPLANZ), different problems occur. In general, ManageWise has difficulty accurately representing the interfaces contained in such nodes. In most

cases, maps are presented properly, but router data shown by selecting *Edit > Database Object* might show too many or too few network interfaces. Interfaces shown without network addresses can usually be deleted manually.

Problems

The following list shows the problems that can occur when the interfaces in a router do not have unique MAC addresses. The problems depend on the ManageWise discovery modules that are loaded, the presence of NetWare servers, and the activities of NetWare LANalyzer Agent software installed on segments. Corrective actions are mentioned but are described more fully in "Corrective Actions" on page 119.

This list assumes a single router with multiple interfaces. Some interfaces are bound to both IP and IPX, some are bound to IP only, and some are bound to IPX only. Only the interfaces in this router are discussed in the list.

◆ **Only NXPIP is running.** Interfaces in the ManageWise database: only IP-bound interfaces are recorded; the MAC address of the interfaces is exactly the same.

Note The duplicated MAC addresses you might see in ManageWise maps and screens depend on the interface vendor, as indicated by the first 3 bytes of the MAC address. For example, a MAC address that starts with 00-00-A2 identifies Bay Networks interfaces; a MAC address that starts with AA-00-04 identifies DECnet interfaces.

Problems: IPX segments are not shown on ManageWise maps.

Corrective Actions: None, if only NXPIP is running. To show IPX segments on ManageWise maps, run NXPIPX.

◆ **Only NXPIPX is running;** NetWare servers are installed on every IPX segment.

Interfaces in the ManageWise database: Only IPX-bound interfaces are recorded; the MAC address of the interfaces is the same.

Problems: IP segments are not shown on ManageWise maps.

Corrective Actions: None, if only NXPIPX is running. To show IP segments on ManageWise maps, run NXPIP.

◆ **Only NXPIPX is running;** NetWare servers are installed on some IPX segments but not on all IPX segments.

Interfaces in the ManageWise database: Only the IPX-bound interfaces to segments with NetWare servers are recorded; the MAC address of the interfaces to those segments is the same. However, the MAC address of interfaces to segments that do not have NetWare servers is 00-00-00-00-00-00.

Note ▼ NetExplorer Manager gives the MAC address 00-00-00-00-00-00 to any interface whose MAC address it cannot identify.

Problems: IPX segments without NetWare servers are not shown in ManageWise maps; IP segments and interfaces are not shown in ManageWise maps.

Corrective Actions: Edit the interface with MAC address 00-00-00-00-00-00 to provide the correct MAC address.

◆ **Only NXPLANZ is running;** NetWare LANalyzer Agent is installed on every segment and each one has discovered some IP addresses on the segment.

Interfaces in the ManageWise database: Only IP-bound interfaces are recorded.

Problems: IPX segments are shown in ManageWise maps, but they have no network addresses; IP and IPX segments connected to the same interface are not consolidated; the router appears as an unknown PC on all the segments connected to the router. In maps, the router does not connect the segments.

Corrective Actions: Consolidate the IP segment and the IPX segment bound to the same interface; delete interfaces with no network address (refer to the Corrective Action labeled "Deleting Interfaces That Have No Network Address" on page 120 and make sure you read the "if and only if" condition).

◆ **Only NXPLANZ is running;** NetWare LANalyzer Agent software is installed on every segment but it does not discover all IP addresses.

Interfaces in the ManageWise database: Interfaces with no network address are recorded; the MAC address of all interfaces is the same.

Problems: No router interfaces have network addresses; the router appears as an unknown PC on each of its segments.

Corrective Actions: Edit the interfaces with no network address (refer to the Corrective Action labeled "Editing the Interface" on page 120 and make sure you read the "if and only if" condition).

◆ **NXPIP and NXPIPX are running;** NetWare servers are installed on every IPX segment.

Interfaces in the ManageWise database: All IP and IPX segments connected to the router are recorded; the MAC address of all recorded interfaces is the same.

Problems: The IP and IPX segments attached to the same interface are not consolidated as one segment; the router appears with more interfaces than it really has.

Corrective Actions: Consolidate the IP and IPX segments bound to the same interface using the Segment Consolidation Tool in the ManageWise program group. Delete an IP interface if the same interface has been discovered with an IPX address, then edit the remaining interface to add the IP address.

◆ **NXPIP, NXPIPX, and NXPLANZ are running;** NetWare LANalyzer Agent is installed on every segment and each one has discovered some IP addresses on the segment.

Interfaces in the ManageWise database: All IP and IPX segments are recorded; the MAC address of all recorded interfaces is the same.

Problems: Router appears with IP interfaces, IPX interfaces, and interfaces with no network address.

Corrective Actions: Delete interfaces with no address (refer to the Corrective Action labeled "Deleting Interfaces That Have No Network Address" on page 120 and make sure you read the "if and only if" condition).

Corrective Actions

Corrective actions you can take are as follows:

◆ Consolidate IP and IPX segments

◆ Delete interfaces that have no network address

◆ Edit interfaces

◆ Delete an interface that has an IP address

Consolidating IP and IPX Segments

Consolidate the IP segment and the IPX segments bound to the same interface.

You can consolidate IP and IPX segments by using the Segment Consolidation Tool. When you use the Segment Consolidation Tool, you select the specific IP and IPX segments to combine.

Deleting Interfaces That Have No Network Address

Delete interfaces that have no network address *only if* the same interface bound to IP or IPX is already discovered.

To delete the interfaces that have no network address, follow these steps:

Procedure ▼

1. **Select the system.**

2. **Select *Edit > Database Object* or click the Edit Object action bar button.**

   ManageWise displays the Database Object Editor.

3. **Select *Adapter Information*.**

   ManageWise displays the adapter information and details for the object.

4. **Select the interface that has no network address, then click Delete.**

5. **Click OK.**

   ManageWise updates the addresses.

6. **Close the dialog box.**

Editing the Interface

Edit an interface that has no network address *only if* the same interface bound to IP or IPX is not discovered.

To edit the interface, follow these steps:

Procedure

1. **Select the system.**

2. **Select *Edit > Database Object* or click the Edit Object action bar button.**

   ManageWise displays the Database Object Editor.

3. **Select *Adapter Information*.**

   ManageWise displays the adapter information and details for the object.

4. **Select the specific interface, and click Edit.**

5. **Enter the IP address or IPX address, or both, of the interfaces, and then click OK.**

   ManageWise updates the addresses.

6. **Close the dialog box.**

Deleting an Interface That Has an IP Address

Delete an interface that has an IP address *only if* the same interface with an IPX address is already discovered. Then edit the remaining interface to add the IP address.

To delete one of the instances of the same interface that has both IP and IPX bound, follow these steps:

Procedure

1. **Select the system.**

2. **Select *Edit > Database Object* or click the Edit Object action bar button.**

   ManageWise displays the Database Object Editor.

3. **Select *Adapter Information*.**

   ManageWise displays the adapter information and details for the object.

4. **Select the IP-bound instance of the interface, and then click Delete.**

5. **Select the IPX-bound instance of the interface, and then click Edit.**

6. **Enter the IP address of the interface, and then click OK.**

   ManageWise updates the addresses.

7. **Close the dialog box.**

   This action could correct the effect that more interfaces are displayed in ManageWise screens than are installed in the router.

Correcting Difficulties with Bridges and Routers

ManageWise does not discover all bridges. ManageWise discovers IP and IPX routers but might not connect them correctly. You can use ManageWise tools, such as the Segment Consolidation Tool, or you can select *Edit > Add* or *Edit > Database Object* to correct your maps so routers and bridges are displayed correctly.

Source Route Bridged Token Rings Displayed Incorrectly

The way ManageWise maps display source-route bridged token rings depends on whether you have NetWare LANalyzer Agent installed on each ring.

◆ If you do *not* have NetWare LANalyzer Agent installed on each ring in your network, ManageWise discovers the network but consolidates all the token rings and displays them as a single segment.

◆ If you *do* have NetWare LANalyzer Agent installed on each ring, each NetWare LANalyzer Agent discovers its own ring (segment) and every system on it. ManageWise displays the ring as an unconnected segment in the internetwork map.

◆ If you have NetWare LANalyzer Agent installed on a ring connected to a router, the ManageWise internetwork map shows the correct connections.

   However, if two networks each have several rings and only one ring in each network is connected to a router, the ManageWise internetwork map shows the correct connections only of the rings

that are connected *directly* to the router. The other source-route bridged rings in each network are displayed as disconnected segments in the internetwork map (see Figure 5-2).

In most cases, the interfaces of the bridge are discovered but the bridge is dismantled and the icon used to represent the bridge is not the bridge icon.

Figure 5-2
When NetWare LANalyzer Agent Is Installed on Each Source-Route Bridged Ring
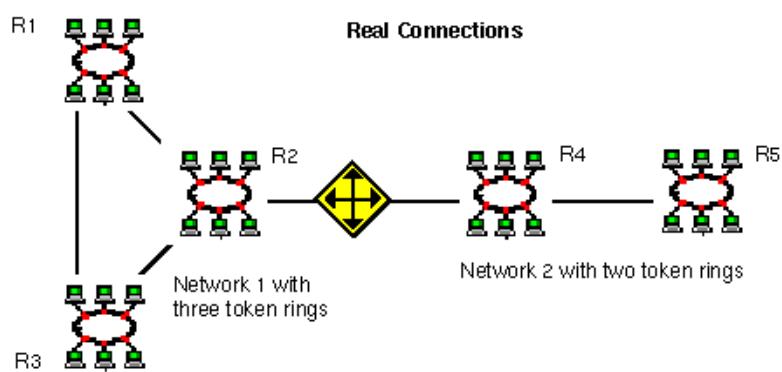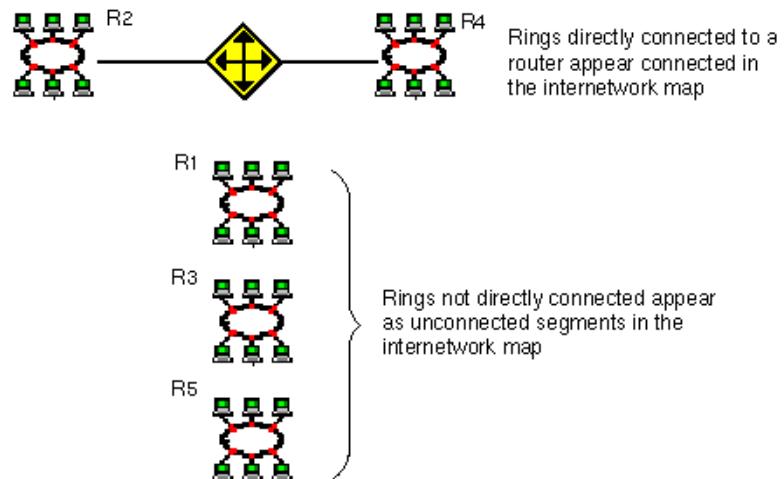
In all these cases, bridge information is not discovered. As a consequence, NetExplorer treats each interface of a bridge as a separate system on the network. One icon appears on the ManageWise maps for each interface of the bridge.

To consolidate the bridge, follow these steps:

Procedure

1. **Record the address of each interface (that is, each icon).**

2. **Delete all the icons except one.**

   See "Deleting Objects" on page 71.

3. **Add interfaces, MAC addresses, and segment connections to the node represented by the remaining icon.**

   3a. **Select *Edit > Database Object*.**

   3b. **Select *Adapter Information*.**

   3c. **Click Add.**

   3d. **Enter the MAC address and IPX network address of one of the interfaces.**

   3e. **Click OK.**

   3f. **Repeat Step 3c through Step 3e for each interface recorded.**

4. **Change the icon to a bridge and add the bridge function.**

   Refer to "Changing the Node Icon" on page 53 and "Adding Services" on page 54.

When you have NetWare LANalyzer Agent installed on one server on each ring of an IPX network, the segment names displayed on the ManageWise internetwork map consist of the IPX network number followed by the MAC address of that server's interface to the ring. If NetWare LANalyzer Agent is monitoring more than one interface, the address shown for a ring is the MAC address of the interface monitoring that ring. Select *Edit > Database Object* to change the names to ones that are more meaningful (refer to "Changing the Node or Segment Name" on page 57).

NetWare MultiProtocol Router Bridge in the Wrong Segment

If you have source-route bridged rings and you have a router with NetWare MultiProtocol Router 2.1 software installed and the router can communicate over IPX, you might find that ManageWise created an extra ("virtual") token ring segment, placed the bridge as the only system in the segment, provided a special MAC address for the bridge, and assigned the segment a name that does not include a MAC address.

When NetWare LANalyzer Agent discovers a token ring, it usually creates a name that has an IP or IPX address followed by the MAC address of the NetWare LANalyzer Agent server.

To make NetWare MultiProtocol Router appear on the correct segment, consolidate the virtual segment with another segment in the same network and, if possible, monitored by the same NetWare LANalyzer Agent.

Use the Segment Consolidation Tool in the ManageWise program group and specify the two segments to consolidate.

Wrong MAC Address for NetWare MultiProtocol Router Bridge

If you have source-route bridged rings and you have a router with NetWare MultiProtocol Router 2.1 software installed and the router can communicate over IPX, you might find that the bridge itself was discovered, but ManageWise gave it an arbitrary MAC address. Select *Edit > Database Object* to correct the MAC address.

Third-Party Routers Connected to the Wrong Segments

ManageWise accurately discovers IP routers when NXPIP.NLM is running on the NetExplorer Server and IP is running on your networks.

However, if IPX is running but IP is not running on your network, ManageWise discovers a third-party router's IPX interfaces only, shows each interface as a separate object on ManageWise maps, and does not show segments as connected by the router.

To consolidate all the interface information for a third-party router and delete the excess objects from a segment map, follow these steps:

Procedure 23

1. **On a ManageWise segment map, find and select one of the objects associated with the router.**

2. **Select *Edit > Database Object*.**

3. **Select *Adapter Information*.**

4. **Click Add.**

5. **Enter the MAC address and IPX network address of one of the *other* router interfaces.**

6. **Enter information about the make and model, if the field is blank.**

   This information is optional.

7. **Click OK.**

8. **Repeat Step 4 through Step 7 for each interface in the router.**

9. **Return to the segment map and delete all the other objects that were associated with this router.**

Routers with Serial Links Not Discovered Accurately

The accuracy with which ManageWise discovers routers connected by serial links depends on whether they are third-party or Novell® routers.

Third-Party Routers

If IP is running on a third-party router and NXPIP.NLM is running on the NetExplorer Server, NetExplorer discovers only the IP-bound interfaces. The router is shown correctly on the ManageWise maps. If IP is not running on a third-party router and NXPIPX.NLM is running, NetExplorer discovers the IPX-bound interfaces. However, these IPX-bound interfaces are not placed in the same router icon on the ManageWise maps. Consequently, the interconnections are not correct in the internetwork map and the router icon appears as multiple separate routers, each containing one network interface from the real router.

To correct the ManageWise information, see "Third-Party Routers Connected to the Wrong Segments" on page 125.

Novell Routers

If both IP and IPX are bound to the router interfaces on both sides of the serial link, ManageWise discovers and displays a discrete IP segment and a discrete IPX segment. It also does not show the IP-bound adapter as the IPX-bound adapter of each router (thus showing an extra adapter for each router).

To correct the ManageWise information, follow these steps:

Procedure **23**

1. **Using the Segment Consolidation Tool in the ManageWise program group, select the two segments to consolidate.**

2. **Select the router on a ManageWise map.**

3. **Select *Edit > Database Object*.**

4. **Select *Adapter Information*.**

5. **Select one of the adapters in the list at the top of the dialog box, and then click Edit.**

6. **In the Edit Adapter dialog box, enter the missing IP or IPX network address information.**

7. **Enter information about the make and model, if the field is blank.**

8. **Click OK.**

9. **In the Adapter Information dialog box, select the extra adapter in the list at the top of the dialog box, and then click Delete.**

10. **Click OK.**

11. **Close the dialog box.**

Now the adapter has both IP and IPX address information and the extra adapter is removed.

Saving NETXPLOR.DAT Files on the NetExplorer Server

For troubleshooting and technical support, you can save one or more copies of the NETXPLOR.DAT file on the NetExplorer Server. You can specify how many copies of the file to store at any time by editing the NETXPLOR.NCF file to add the /B option to the command line that loads NETXPLOR. The command line is as follows:

```
LOAD SYS:\NMDISK\NETXPLOR /B count
```

By default, NETXPLOR makes no backup copies of the NETXPLOR.DAT file. If you use the /B option, NETXPLOR makes a backup copy each time NETXPLOR.NLM is unloaded and stores the copy in the SYS:\NMDISK\DATSAV directory. If the number of copies has reached the value of *count,* NETXPLOR overwrites the oldest copy. If you have set the value of the count parameter and later you want to reduce it, you must erase the copies in the DATSAV directory.

Note The NETXPLOR.DAT file is a sequential record file that holds the ManageWise network discovery data. *This file should be excluded from server backup* (because it is usually open). If you use the /B option, the file is backed up automatically whenever NETXPLOR.NLM is unloaded. The file is created fresh whenever NETXPLOR.NLM is loaded again.

part **IV** *Handling Alarms*

ManageWise® software provides an alarm system that you can use to alert you to errors (such as an inability to connect to a device) or other conditions (such as a high utilization rate) on the network. You can configure how ManageWise responds to alarms, and even set it up to launch selected programs when events occur. This part of the guide contains two chapters:

◆ Chapter 6, "Understanding Alarms" on page 131, explains the approach ManageWise uses to alarms. Included is a discussion of alarm characteristics, alarm indicators, and how to display and handle logged alarms.

◆ Chapter 7, "Network and Device Alarms" on page 153, explains how ManageWise uses alarms for specific devices. This chapter goes into detail about alarms for servers, segments, and hubs.

chapter

6 *Understanding Alarms*

ManageWise® software alerts you to network conditions that are useful to know about or that require action. It does this in the course of handling alarms that it receives from various systems and devices on the network, as illustrated in Figure 6-1.

The ManageWise Console receives network alarms if Alarm Manager and SNMP Data Server or NetExplorer™ Manager are running. Multiple alarm sources are handled by the system; each source is considered an alarm family.

NetWare® Management Agent™ software, NetWare LANalyzer® Agent™ software, LANtern™ network monitors, and many network devices support SNMP and might send SNMP traps to the ManageWise Console. ManageWise can receive traps and process them as alarms. Any SNMP trap received by the ManageWise Console is forwarded to the Alarm Manager for handling.

Note ▼ Not all server alarms can be configured using the NWTRAP.CFG file. Rather, only those that are included in NWALARM.MIB can be configured. For example, alarms generated by setting thresholds at the ManageWise Console cannot be configured from NWTRAP.CFG.

Figure 6-1
Overview of Alarm Handling
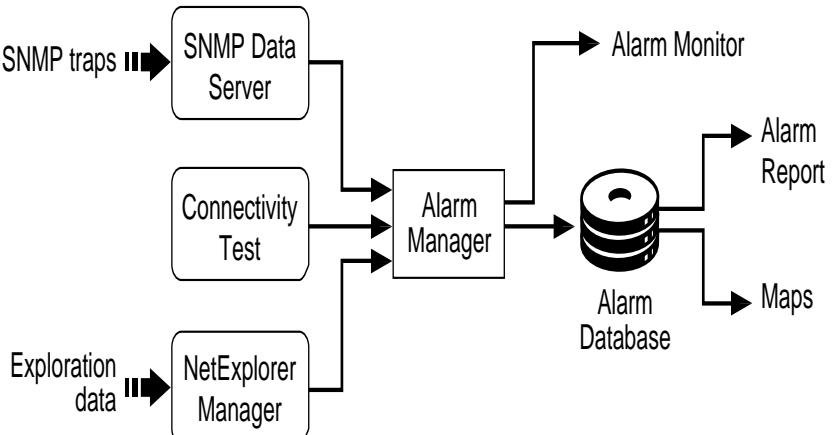
When Alarm Manager receives an alarm, it needs to know what to do in response to the alarm. ManageWise might perform actions such as these:

◆ Save the alarm to the database

◆ Sound an audible beep

◆ Execute a program

◆ Display a ticker-tape message

The way ManageWise responds to alarms is shown by its *alarm disposition*, and Alarm Manager deals with all alarms consistently, based on default and user-configured dispositions.

This chapter discusses alarm characteristics and alarm dispositions. It also explains how you can display real-time information about all alarms and handle saved alarms.

Alarms Recognized by ManageWise

ManageWise recognizes the following kinds of alarms:

- **NetExplorer alarms** alert you to events in the network discovery process and do not usually represent problems. These alarms can occur any time during discovery.

- **Connectivity Test alarms** are generated by the ManageWise Console when using the Test Connectivity facility.

- **SNMP alarms** are generated by agents that support SNMP. For information about preparing ManageWise to interpret SNMP alarms, refer to "Getting Started" on page 317.

- **Unknown alarms** are alarms received from unknown sources, such as a MIB that is no longer use, but is still in the \CURRENT directory.

Alarm Characteristics

Each ManageWise alarm represents a specific condition and has configurable characteristics. Default characteristics are assigned by ManageWise, but you can change them:

- ◆ **Severity**—ManageWise severity levels are listed in Table 6-1.

- ◆ **Object state of the segment or device affected by the alarm**—For example, whether a segment or device is *operational* or *not operational.*

- ◆ **Dispositions**—Ways ManageWise records and responds to alarms of a particular type.

Table 6-1
Levels of Alarm Severity

Severity Level	Definition
Critical	Urgent problem requiring immediate action to avoid further degradation of the affected object and possibly many affected objects.
Major	Serious problem requiring prompt attention to avoid further degradation of the affected object and possibly a small number of associated objects.
Minor	Problem to be addressed under normal work schedules.
Informational	Lowest level of priority, indicating that the alarm is sent for information only and no action is required. The information might be useful for other purposes, such as supporting trend analysis and planning.
Unknown	Information that might be of interest or might be the source of a problem or indicating that ManageWise is not able to interpret the event.

Alarm Indicators

You can monitor the network for alarm-triggering events by observing the status bar, maps, and the Alarm Monitor and Alarm Report tables. Table 6-2 lists the alarm indicators and explains what type of alarm each indicator applies to.

Table 6-2
Alarm Indicators

Alarm Indicator	Applies To
Bell icon on maps that include the affected object	Alarms with critical, major, and minor severity that were logged.
Dimmed object icon on maps	Alarms for a condition that, according to ManageWise, renders a device inoperative.
Bell icon on status bar	All alarms.
Ticker tape on status bar	Alarms with the option set to ticker tape. These are mostly alarms with critical severity.
Alarm displayed in Alarm Report	Alarms saved to the database.
Alarm displayed in Alarm Monitor	400 most current alarms.
Other action specified by you for a disposition	Alarms with a user-customized disposition.

Alarms on the Status Bar

ManageWise automatically displays alarm icons and alarm messages on the status bar. Upon recognizing an alarm-triggering event, ManageWise displays an alarm icon (a bell) at the left end of the status bar (refer to Figure 6-2). In addition, the ticker-tape field displays a message describing the alarm if the severity is critical or if you selected Ticker Tape in the Alarm Disposition (refer to "Changing Alarm Dispositions" on page 137).

Figure 6-2
Alarm Indicators on the Status Bar

Alarm icon   Ticker tape field   Date   Time
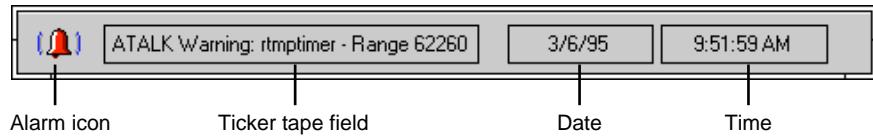
Alarms on Maps

Alarms are represented on maps by an alarm icon (a bell), shown in Figure 6-3. For each alarm, a bell is displayed above each affected segment or device until you acknowledge all alarms outstanding against that object.

Figure 6-3
Alarm Indicators on an Internetwork Map

Critical Alarm: Red Bell, left side of Alarm Bar

Major Alarm: Magenta Bell, center of Alarm Bar

Minor Alarm: Yellow Bell, right side of Alarm Bar
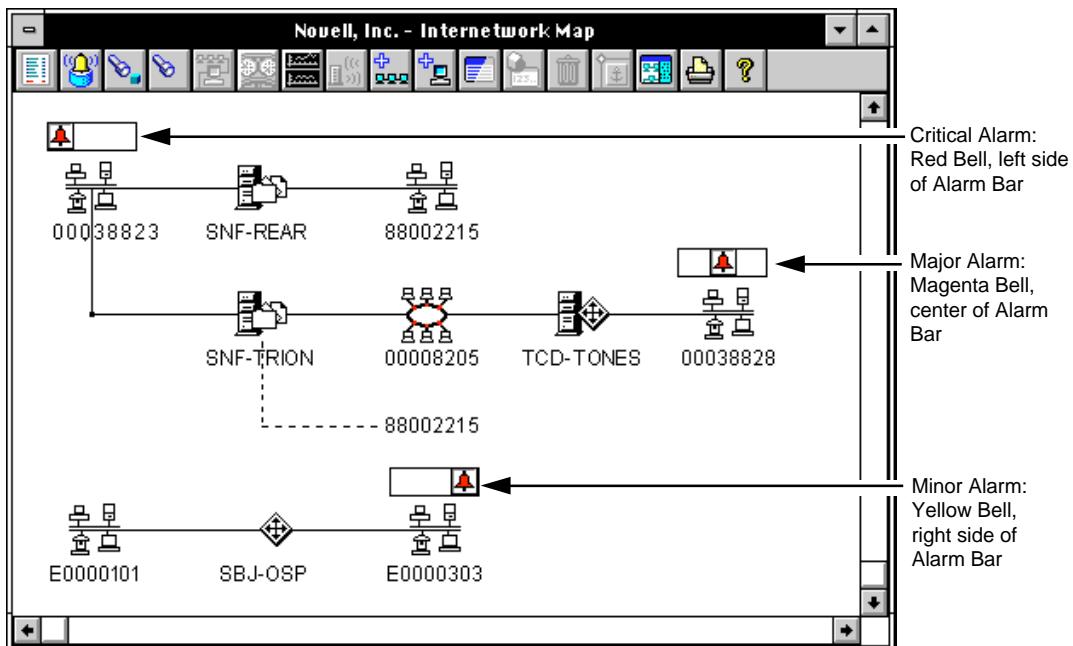
To be displayed on maps, an alarm must have a severity level of critical, major, or minor. The color of the bell and its position above the object indicates the level of alarm severity, as explained in Table 6-3.

Note In addition to displaying alarms on maps, ManageWise saves alarms to the database.

Table 6-3
Bell Icons and Alarm Severity Levels

Alarm Severity Level	Bell Color	Bell Position
Critical	Red	Left of the object
Major	Magenta	Center of the object
Minor	Yellow	Right of the object

If one or more of the devices on a segment has an alarm, a single bell icon appears next to the segment icon. The color and position of the bell indicates the most severe alarm on the segment. For example, one segment in Figure 6-3, 00038823, has a bell icon indicating a critical alarm. Therefore, unless the alarm relates to the segment itself, the segment has one or more devices with alarms of critical severity or less.

Changing Alarm Dispositions

ManageWise provides the Alarm Disposition table listing the characteristics of your alarms. You can change the way ManageWise deals with alarms when they are detected. For example, you might consider an alarm less severe than the defaults attributed to it, or you might want to save the alarm to the database, or you might want to specify a new file to execute.

Table 6-4 lists the columns in the Alarm Disposition table and explains the information given in each.

Table 6-4
Alarm Disposition Table Columns

Column	Contents
Category	Lists the kind of alarm: NetExplorer, Connectivity, or SNMP MIB.
Type	Lists the alarm. The Type list includes alarms about networks, segments, routers, servers, and workstations; server disks, volumes, directories, memory, and performance; and other objects tracked by ManageWise.
Severity	Lists how critical the alarm is. Refer to Table 6-1 on page 134 for an explanation.
State	Operating state of the object: Operational, Nonoperational, Degraded [partly operational], and Unknown.
Save in Database	Indicates whether the alarm is saved in the database.
Beep	Indicates whether to sound a beep at the ManageWise Console when the alarm appears.
TIcker Tape	Indicates whether to display an alarm summary in the ticker-tape field.
Launch a Program	Indicates whether the alarm launches a program. See "Program to Be Launched," which follows.
Program to Be Launched	Program to launch (if enabled) when the alarm appears.

Displaying Real-Time Information about All Alarms

ManageWise includes the Alarm Monitor, which is a real-time display for alarms that occurred since you started ManageWise (or since you restored the Alarm Manager, if you closed it).

To display the Alarm Monitor, select *Fault > Alarm Monitor.*

Figure 6-4 shows the Alarm Monitor.

Figure 6-4
Alarm Monitor
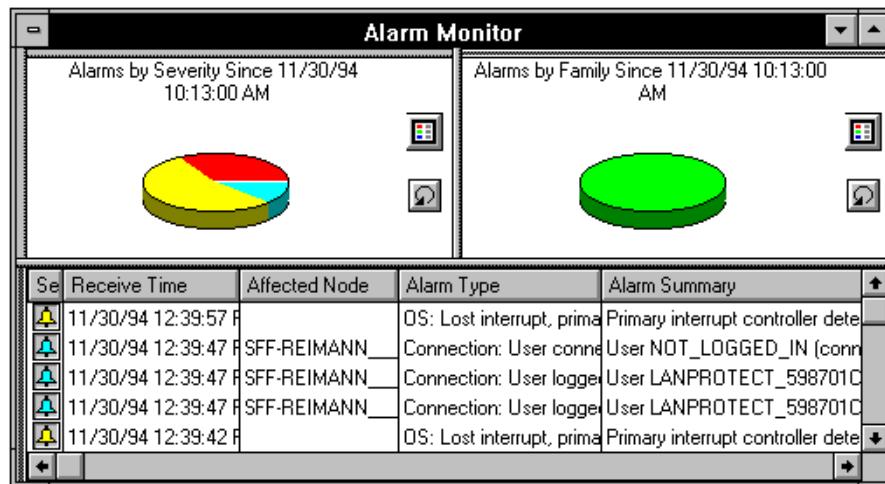
The top pane of the Alarm Monitor window contains pie charts of alarms collected since Alarm Manager started. Alarms are broken out by severity and by family and updated every two minutes. To the right of each pie chart are control buttons.

The bottom pane of the Alarm Monitor window displays a table of detailed information about the last 400 alarms, updated whenever a new alarm occurs. New alarms are added at the top of the table.

Table 6-5 describes the Alarm Monitor fields. You can print and export data from the table and pie charts,

Table 6-5
Alarm Monitor Fields

Field	Explanation
Receive Time	Date and time when the ManageWise Console received the alarm.
Alarm Type	Generic description of the alarm—for example, Volume out of disk space.
Affected Node	Segment or device affected by the alarm.
Alarm Summary	Summary of the event, often including the name or address of the object affected by the alarm.
Station Type	Type of the affected station, as defined in the database—for example, router or Ethernet segment.
Severity	Severity level that you attribute to the alarm.
State	Operating state that you attribute to the object affected by the alarm.
Agent Address	Network address of the device that sent the alarm to ManageWise.

Unknown Alarms

ManageWise reports an unknown alarm when devices on the network issue alarms pertaining to MIB files that are not compiled and the relevant alarm traps are not integrated into the ManageWise database TRAPS.BTV file. To correct this problem, copy MIB files you want to compile from the \MW\NMS\SNMPMIBS\ALLMIBS directory to the \MW\NMS\SNMPMIBS\CURRENT directory, and then run the SNMP MIB compiler. If the MIB file pertaining to the device generating the unknown alarm is not available, contact the manufacturer of the device to obtain the MIB file.

Note We recommend that you keep a copy of all the MIB files you acquire in the \MW\NMS\SNMPMIBS\ALLMIBS directory.

Copying MIB files from the \MW\NMS\SNMPMIBS\ALLMIBS directory to the \MW\NMS\SNMPMIBS\CURRENT directory might cause ManageWise MIB compilation errors. The following are errors that you might encounter:

◆ Redefinition of errors can be generated by the MIB compiler if it compiles older version MIB files. This occurs when a newer version of the MIB file exists in the \MW\NMS\SNMPMIBS\CURRENT directory under another name. You must decide which version to compile and delete the other file from the \MW\NMS\SNMPMIBS\CURRENT directory before compiling again.

◆ Undefined errors can be generated by the MIB compiler if you compile a MIB file that depends on other MIB files that are not compiled. To satisfy all dependencies in the MIB files being compiled, verify that all MIB files referenced in the IMPORTS section of the MIB file are included in the \MW\NMS\SNMPMIBS\CURRENT directory.

Displaying and Handling Logged Alarms

The Alarm Report displays information about alarms that are saved in the ManageWise database. You can display multiple Alarm Reports, with each either handling alarms for objects you have selected on maps or all alarms stored in the database.

To display an Alarm Report, follow these steps:

Procedure

1. Limit the alarms represented on the Alarm Report, if desired.

   1a. Remove all selected objects on the active map by selecting *Edit > Deselect All* or pressing Esc**.**

   1b. On the current active map, select one or more objects for which you want alarm information.

If you select a segment, the Alarm Report displays all alarms for that segment and all devices on it.

2. Select *Fault > Alarm Report*.

ManageWise displays the Alarm Report (refer to Figure 6-5). It lists all alarms stored in the database for the objects you selected.

Figure 6-5
Alarm Report

Understanding the Alarm Report

The Alarm Report gives you detail information about each alarm it receives. You can use this information to understand the source of problems and prepare to solve them, if needed. Table 6-6 explains the Alarm Report fields.

Table 6-6
Alarm Report Fields

Field	Explanation
Severity	Severity level that you attribute to the alarm condition.
Ack'd	Indicates that you acknowledged the alarm.
Note	Indicates that you entered notes about the alarm.
Receive Time	Date and time ManageWise received the alarm.
Affected Node	Segment or device affected by the alarm.

Table 6-6 *continued*
Alarm Report Fields

Field	Explanation
Type	Generic description of the alarm—for example, Volume out of disk space.
Summary	Summary of the event, often including the name or address of the object affected by the alarm condition.
Node Type	Type of the affected station, as stored in the database—for example, router or Ethernet segment.
State	Operating state that you attribute to the object affected by the alarm condition.
Agent Address	Network address of the device that sent the alarm to ManageWise.
Ack'd Time	Date and time you acknowledged the alarm.

Viewing the Alarm Report Summary Pane

Because the Alarm Report displays so much information in a limited amount of space, it sometimes requires you to scroll and resize the columns to see all the data. To make the information more accessible, the Alarm Report window has a summary pane at the bottom. This pane lets you select an alarm and see all the details shown in the columns of the Alarm Report at a glance. You can also copy this data to the Clipboard.

Scrolling Alarm Reports

ManageWise adds new alarms to the Alarm Report by adding new rows at the top of the table. If ManageWise fills the window with new alarms, the scroll box moves down and the new alarms are not visible. To display the new alarms, move the scroll box up. To move the scroll box to the top, press the Home key. To move the scroll box to the bottom, press the End key.

Displaying Help about an Alarm

You can bring up context-sensitive help about any alarm in the Alarm Report. You can also add notes to a help topic by selecting *Edit > Annotate* in the menu bar of the help window.

Going to the Device Affected by an Alarm

You can use the Alarm Report to go to the device affected by a selected alarm. Finding a device displays and selects its icon on an internetwork map, segment map, or custom map.

Note ▼ ManageWise cannot display devices that are filtered or deleted from a segment map. If you want to search for a filtered device, first bring it back to the map by selecting *View > Filter By*, then rerun the `Go To` command. Any device you want to find must also be registered in the ManageWise database.

To find an affected device on a map, follow these steps:

Procedure ▼

1. **Select the alarm in the Alarm Report.**

2. **Click the button labeled with the Locate icon.**

   ManageWise displays the Locate in Selected Map dialog box.

3. **Select the desired map, then click the Locate button.**

   ManageWise opens the map, displays the object, flashes a box around the icon, and selects it. You can now gather the following information about the object:

   ◆ Check whether the icon is dimmed and the object is operational

   ◆ Test the connectivity of the object to the network

Acknowledging Alarms in the Alarm Report

Alarms appear on all maps containing the object that generated the alarm. When you acknowledge an alarm, your acknowledgment is recorded in the Alarm Report and the associated alarm bitmaps are removed from maps.

To acknowledge one or more alarms in the Alarm Report, follow these steps:

Procedure ▼

1. **If you want to acknowledge all alarms, click the Check Mark-All button. Otherwise, go to Step 2.**

2. **Select the alarms you want to acknowledge.**

3. **Click the Check Mark button, or select** *Fault > Ack Alarms***, or press** Control+A**.**

    ManageWise takes the following actions:

    ◆ Removes acknowledged alarms from all maps.

    If a segment includes devices with unacknowledged alarms, a bell remains on the map above the segment icon. If the remaining alarms are of a lower severity than the acknowledged alarm, the bell changes color and position. If no unacknowledged alarms remain on that segment and its devices, the bell disappears.

    ◆ Saves the date and time of the acknowledgment to the database and displays it in the Ack'd Time column.

    ◆ Places a check mark in the Ack'd column for the alarm entry in all Alarm Reports.

Note ▼ Alarm acknowledgments are background operations; you might experience a delay between clicking the button and seeing alarms acknowledged. During this time, you can proceed with other ManageWise or Windows operations.

Acknowledging Alarms on a Map

To acknowledge alarms on a map, follow these steps:

Procedure ▼ 23
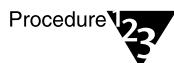
1. **Select one or more alarm icons on a map.**

2. **Select** *Fault > Ack Alarm***.**

    Alternatively, you can press Control+A. When the acknowledgments are complete, ManageWise displays a check mark next to acknowledged alarms and displays a message box to tell you the acknowledgments are complete. All bell icons for the selected objects, and any objects they contain, disappear from the maps unless new alarms have arrived in the interim.

Note ▼ Alarm acknowledgments are background operations; you might experience a delay between clicking the button and seeing alarms acknowledged. During this time, you can proceed with other ManageWise or Windows operations.

Adding Notes to the Alarm Report and the Database

You can add, edit, and delete notes about alarms listed in an Alarm Report. When an alarm includes a note, the Note icon appears beside the alarm entry in the Note column.

To add a note about an alarm, follow these steps:

Procedure

1. **Select the alarm on the table.**

2. **Click the button with the Note icon.**

   The system displays the Alarm Notes dialog box.

3. **Enter, edit, or delete the note.**

   A note can contain as many as 255 characters.

4. **Click OK.**

   The Note icon appears in the Note column—the column labeled with a Note icon for the alarm entry—on all Alarm Reports.

Deleting Alarms

You can delete one or all alarms listed on the active Alarm Report. The deletion removes the alarms from all Alarm Reports, all maps, and the database. Any alarm notes are deleted automatically with the alarms.

Note

You can delete all alarms or only selected alarms based on their severity or age by using the Database Administration Tool, explained in "Deleting Selected Alarms" on page 147. Doing so enables you to keep selected alarms based on their characteristics. However, to use the Database Administration Tool, you must first exit ManageWise.

To delete alarms listed in an Alarm Report, follow these steps:

Procedure

1. **Select the alarm.**

   If you are deleting all of the alarms, skip this step and proceed to Step 2.

2. **Click Delete or Delete All.**

ManageWise removes deleted alarm bitmaps from the internetwork map, all segment maps, and custom maps.

If you delete an alarm for a device but the device includes other devices with alarms, a bell remains on the map above the segment icon. If the remaining alarms are of a lower severity than the deleted alarm, the bell changes color and position. If acknowledged alarms, or alarms with a severity no higher than minor, remain on that segment or its devices, the bell disappears.

Note ▼ Alarm deletions are background operations; you might experience a delay between clicking the button and seeing alarms disappear from maps and Alarm Reports. During this time, you can proceed with other ManageWise or Windows operations.

Deleting Selected Alarms

The Alarm System includes two alarm log files—EVENT.BTV and EVCOMENT.BTV. The EVENT.BTV file increases in size each time ManageWise logs an alarm. The EVCOMENT.BTV file increases in size each time you add a note using the Alarm Report.

Both alarm log files can increase in size until they fill your hard disk. If you are running out of disk space or if the time required to display the Alarm Report table becomes objectionably long, you need to delete logged alarms.

You should delete logged alarms periodically to reduce the size of the alarm log files as well as reduce the number of alarms in the database. Before deleting alarms, you should make a copy of your existing database (refer to "Maintaining the ManageWise Database" on page 92).

To delete selected alarms, follow these steps:

Procedure ▼ **1. Start the Database Administration Tool as described in "Starting the Database Administration Tool" on page 92.**

2. Select *Delete Selected Alarms*.

The ManageWise DB Admin dialog box is displayed.

This dialog box gives you the following options:

◆ Delete all alarms logged in the database.

◆ Delete alarms selectively

—Delete all alarms logged in the database before a given date and time.

—Delete all alarms logged in the database with a severity less than or equal to a given severity.

—Delete all alarms logged in the database before a given date and time *and* with a severity less than or equal to a given severity.

If you select the first option and delete all alarms logged in the database, the alarm log files are reduced to a minimum size. If you select any of the other options and delete alarms selectively, the alarm log files are not reduced in size. The records are simply marked as empty and filled with new data as it arrives.

3. **To delete alarms, click the appropriate option button and check boxes, and then click OK.**

Launching Programs in Response to Alarms

You can set up ManageWise to launch programs automatically when selected alarms arrive. This allows you to identify alarms that require special attention or a special response and ensure that they receive it. For example, when particularly severe alarms are generated, you might want to launch a program that sends a message to a pager calling the system administrator.

Note ManageWise supplies the capability to launch programs, but does not supply any predefined programs. However, these can be written as Windows .PIF and .EXE files and DOS .EXE, .BAT, and .COM files.

In addition to telling ManageWise which program to launch, you can also specify parameters to pass to the program. You can pass literal parameters and replaceable parameters:

◆ *Literal* parameters are passed directly to the program. Any text is not parsed but is read as literal text strings.

◆ *Replaceable* parameters (refer to Table 6-7) are replaced with the desired information. They must be preceded by a percent (%) sign.

The percent sign can be followed by an optional length field to limit the length to which the parameter can expand.

Table 6-7
Replaceable Parameters

Parameter	Name	Description
a	Alarm ID	Identification number of the alarm as it is stored in the database.
c	Affected class	Class of equipment that sent the alarm. Can be any portion of the network; categorized for database indexing.
o	Affected object number	Identification number of the device that generated the alarm as it is stored in the database.
s	Alarm summary string	Message describing the alarm. Same as the status bar ticker-tape message.
t	Alarm type string	Description of the alarm; matches the Alarm Type column in the Alarm Report.
v	Severity number	Alarm severity: 1 = critical 2 = major 3 = minor 4 = informational All others are 0, unknown.

ManageWise does not specify a separator between the parameters: use the separator specified by the program. Any parameter not recognized is passed as a text string.

To launch programs in response to alarms, follow these steps:

Procedure **23**
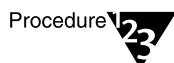
1. **Select one or more alarms for which you want to launch a program and display the Edit Alarm Disposition dialog box.**

   "Changing Alarm Dispositions" on page 137 explains how to do so.

2. **Fill in the fields, as desired.**

3. **Click the Launch Program check box and the Save in Database check box.**

When you launch a program, you must also save it in the database.

4. **Specify the full pathname of the program to execute by clicking in the Program box and using the Browse button to find it.**

   Before expansion, this text must be fewer than 127 characters, including the full pathname. You can specify Windows .PIF and .EXE files and DOS .EXE, .BAT, and .COM files.

5. **Click the Parameters box and specify any replaceable parameters (from Table 6-7) or literal parameters you want to pass to the program.**

   Before expansion, this text must be fewer than 140 characters.

   After full expansion, the combination of Program and Parameters must not exceed 120 characters, including spaces. If it does, the replaceable parameters are truncated first, then the text you enter.

6. **Click OK.**

   Repeat this procedure for any other programs you want your alarms to launch.

The next time that alarm is received, ManageWise launches the program you selected.

The sample command in Figure 6-6 launches a program called Pager, located in the C:\ directory, and passes a phone number, the Alarm Summary string (limited to 40 characters), and the Alarm type string.

Figure 6-6
Sample Command Launch

Program: C:\PAGER\PAGER.EXE   Browse

Parameters: 408-555-4321 %40s %t

Comment
Program parameters to be passed when launch program is activated. %a - Alarm object ID, %c - affected Class, %o - affected Object id, %s - Summary string, %t - Type string, %v - seVerity number.
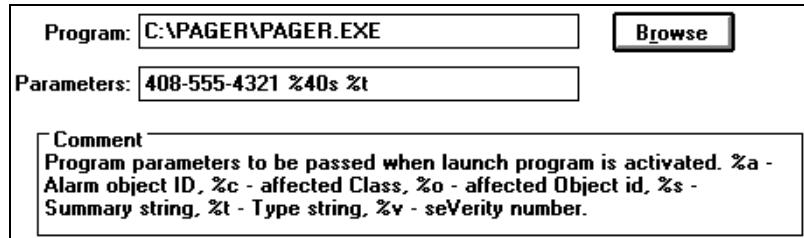
Printing Alarm Data

ManageWise lets you print data from the Alarm Disposition window, Alarm Report window, and Alarm Monitor window. To print data from the Alarm Disposition window or Alarm Report window, follow these steps:

Procedure

1. Select the alarms you want to print.

To select multiple alarms, hold down the Ctrl key and click on additional alarms.

2. Click the Print action bar button or select *File > Print*.

A print dialog box appears. You can choose to print either all of the alarms listed by clicking All or the alarms that you selected in Step 1 by clicking Selection.

3. Click OK.

The alarms you chose are printed.

To print data from the Alarm Monitor window, follow these steps:

Procedure

1. Select the window pane you want to print.

If you select the alarm table in the bottom pane, select the alarms that you want to print.

2. Select *Edit > Print*.

If you selected a window pane containing a pie chart in Step 1, selecting *Edit > Print* prints the pie chart. If you selected the bottom pane containing the alarm table, a print dialog box appears. Follow these steps to print the alarm table:

2a. Select either All or Selection.

All prints all of the entries in the alarm table. Selection prints the alarms that you selected in the bottom pane of the Alarm Monitor window.

2b. Click OK.

For a more detailed explanation of how to print, refer to *ManageWise 2.6 Setup Guide*.

Exporting Alarm Data

ManageWise lets you export data in an Alarm Report or Alarm Monitor using either the Export button in the action bar or by selecting *File > Export*. For a more detailed explanation of how to export data, refer to *ManageWise 2.6 Setup Guide*. After exporting alarm data, you can use a spreadsheet and third-party software to filter, display, and print data.

chapter **7** *Network and Device Alarms*

ManageWise® software helps you identify problems with your network and the devices on it. Refer to Chapter 6, "Understanding Alarms," for information about the ManageWise alarm strategy. This chapter contains the following sections, which explain the specific kinds of alarms that alert you to conditions on the network:

◆ "Server Alarms" on page 153.

◆ "Segment Alarms" on page 154.

Note ManageWise displays alarms in the standard Windows format.

Server Alarms

This section explains how you can set thresholds for server alarm parameters. Two types of thresholds are supported: rising thresholds and falling thresholds. An alarm parameter can have either a rising or a falling threshold, but not both.

◆ **Rising threshold**—Used for parameters that you expect to stay below a certain value. The ManageWise server sends alarms if the parameter rises above the threshold. The icon shown below represents a rising threshold.

◆ **Falling threshold**—Used for parameters that you expect to stay above a certain value. The ManageWise server sends alarms if the parameter falls below the threshold. The icon shown below represents a falling threshold.

You can set the alarm threshold for any selected parameter. For more information about alarms, refer to Chapter 6, "Understanding Alarms." For information about printing, exporting, and copying data, refer to *ManageWise 2.6 Setup Guide.* For more information about servers, refer to Chapter 8, "Managing Servers."

Segment Alarms

You can configure the NetWare LANalyzer® Agent™ software to send alarms in response to events on the segments. These alarms are sent to the ManageWise Console, which displays the alarms and gives you mechanisms for acknowledging them. Refer to Chapter 6, "Understanding Alarms," for a full explanation of how to manage alarms.

This chapter gives you the following information about alarms:

◆ Which alarms ManageWise supplies for Ethernet, token ring, and FDDI segments

◆ How to set the alarms

Setting alarm thresholds frees you from having to constantly monitor segments for problems. Logging alarms enables you to keep historic data about the performance of the network.

Chapter 13, "Analyzing Your Network," describes many of the statistics for which you can set alarm thresholds.

Setting Segment Alarm Thresholds

ManageWise lets you set alarm thresholds for Ethernet, token ring, or FDDI statistics on each segment and sends an alarm every time the statistic on that segment exceeds the threshold in the selected interval. This is called a *rising alarm* because it is sent only when the threshold is

exceeded while the statistic is rising. All segment alarms are reported as rising alarms.

Before setting a threshold, use the Segment Graph window to observe your average and peak traffic levels. Then choose thresholds high enough to avoid repeated alarms under normal network conditions, yet not so high that significant network problems go undetected. To prevent multiple alarms caused by the same condition, network performance must fall at least 10 percent below the threshold value and then rise above the threshold again before the software records the same alarm.

Note **▼** ManageWise provides default values for alarm thresholds but does not enable them. You can and should enable the alarms and then change the default threshold values, depending on your network environment.

When setting alarm thresholds, you specify the following factors:

◆ Statistic

◆ Value of the statistic

◆ Sampling interval

When the value of the statistic exceeds the selected value in the selected interval, ManageWise generates an alarm.

You can also disable all alarms or one alarm. To do so, click the Disable button in the Selected Object Configuration dialog box or edit a single statistic and click the Disable button in the Set Alarm dialog box. Save the value as usual.

V *Maintaining Your Network and Its Devices*

ManageWise® software lets you monitor and manage any network devices and segments on which the right agents are installed. In addition, you can use the ManageWise Console to check for connectivity of any device, manageable or not.

This part of the guide contains the following chapters:

◆ Chapter 8, "Managing Servers" on page 159, explains the kinds of information you can display about servers, how you can collect trend data to use for planning or troubleshooting, and how to use tools to modify a server's configuration.

◆ Chapter 9, "Managing Workstations" on page 225, explains how to display workstation configuration and performance information and suggests ways to use the information.

◆ Chapter 10, "Managing Routers" on page 237, explains how to access router traffic statistics, monitor IPX™ routers, view pathways between routers, and monitor NetWare® Link Services Protocol™ (NLSP™) routers.

◆ Chapter 11, "Managing Hubs" on page 265, explains Novell's management strategy for hubs that comply with the Novell® Hub Management Interface™ (HMI™).

◆ Chapter 12, "Managing SNMP Devices" on page 317, explains how to use ManageWise to manage devices that have been instrumented to SNMP.

◆ Chapter 13, "Analyzing Your Network" on page 339, explains how to use ManageWise tools to monitor segment performance and capture and decode packets for segments connected to servers with NetWare LANalyzer® Agent™ software installed.

◆ Chapter 14, "Testing Connectivity" on page 411, describes the ManageWise tools used to verify connections between devices on the network.

◆ Chapter 15, "Managing Network Addresses" on page 419, explains how to use ManageWise to list network numbers and addresses for possible use in setting up and troubleshooting your network.

chapter **8** *Managing Servers*

From the ManageWise® Console, you can monitor and manage NetWare® servers on your internetwork. You can monitor the state of a server over various periods of time by keeping trend data. Using trend data, you can plan future expansion of servers (increasing volume and disk sizes or increasing the number of users allowed access to the server at one time, for example). In conjunction with setting trend thresholds, you can use ManageWise to troubleshoot server problems on your internetwork (suddenly there is very little free space on a server's volume, for example).

You can also view parts of the server when troubleshooting a problem. Viewing parts of a server's configuration (the server's network interfaces, for example) might help you solve the problem with the server.

To help you manage servers, volumes, print queues, and users, you can run NetWare Administrator utilities without leaving the ManageWise Console. NetWare Administrator is available to you from the action bar.

The ManageWise Console also provides a graphical user interface for the NetWare SET utility. Using the SET utility, you can view and configure a server's operating system parameters to improve the performance of that server.

For more information about NetWare Administrator and the SET utility, refer to your NetWare server documentation.

NetWare Management Agent™ software installed on servers makes it possible for the ManageWise Console to display server performance and configuration data. This chapter describes managing servers that have NetWare Management Agent 2.x installed.

This chapter contains the following sections:

◆ "Monitoring Print Servers" on page 160.

◆ "Monitoring File Servers" on page 164.

◆ "Monitoring Trends" on page 204.

◆ "Viewing Trends" on page 212.

◆ "Setting Trends and Thresholds" on page 216.

◆ "SET Server Parameters" on page 220.

Monitoring Print Servers

Because ManageWise enables you to see the relationships between NetWare file servers, print servers, print queues, and printers, you can see the complete path that print jobs must take to go from a network station to a printer.

This makes it easy to follow the path of a failed print job and determine the point at which it failed. Because it's easy to see how your network print services are configured, it's easy to optimize the configuration by balancing the number of print queues per print server and the number of print servers per file server. ManageWise contains a NetWare utility that enables you to get information concerning NetWare print servers.

To report the activity in the print server, follow these steps:

Procedure

1. Select *View > All > NetWare Print Servers.*

The All NetWare Print Servers window, shown in Figure 8-1, is displayed.

Note

The list of print servers shown in the All NetWare Print Servers window can either display only print servers in the database or display print servers in the database and print servers found dynamically. To set what is displayed, refer to *ManageWise 2.6 Setup Guide*.

Figure 8-1
All NetWare Print
Servers Window
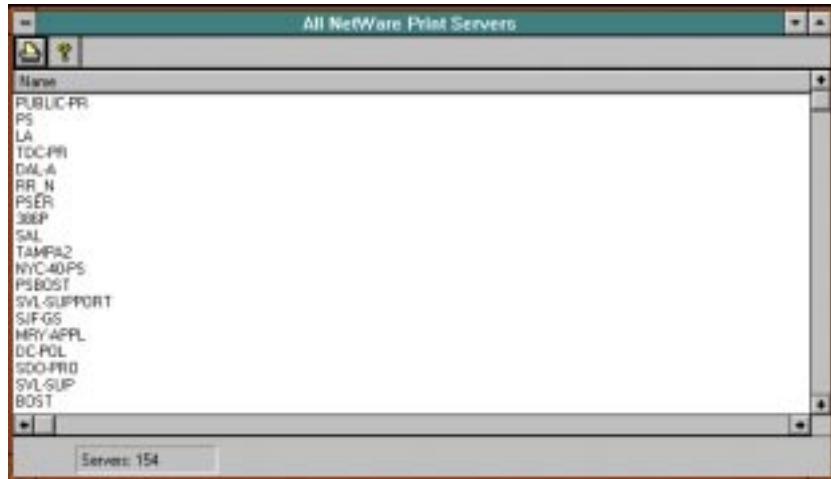
2. **Double-click a print server.**

   Alternatively, you can do one of the following:

   ◆ Select a specific server, and then select *File > Open > Print Server*.

   If you use the menu command, a dialog box appears. You specify the server by IPX™ address.

   ◆ Double-click the target server icon while viewing an internetwork map, segment map, or custom map.

   ManageWise automatically tries to log in to one of the file servers serviced by this print server, using GUEST as the username, to obtain printer information about the print server. If this automatic login fails, the Print Server Configuration login dialog box, shown in Figure 8-2, appears and prompts you to log in to one of the file servers, using your own username and password.

Figure 8-2
**Print Server
Configuration Login
Dialog Box**
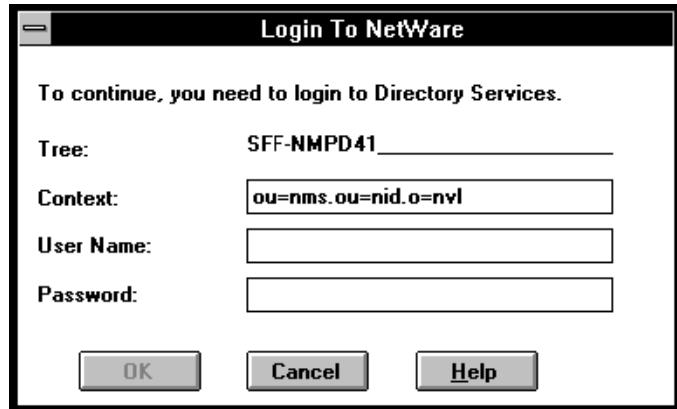
If the Print Server Configuration login dialog box appears, enter your username and password, and then click OK. The Print Server Configuration window, shown in Figure 8-3, is displayed.

Figure 8-3
**Print Server
Configuration
Window**
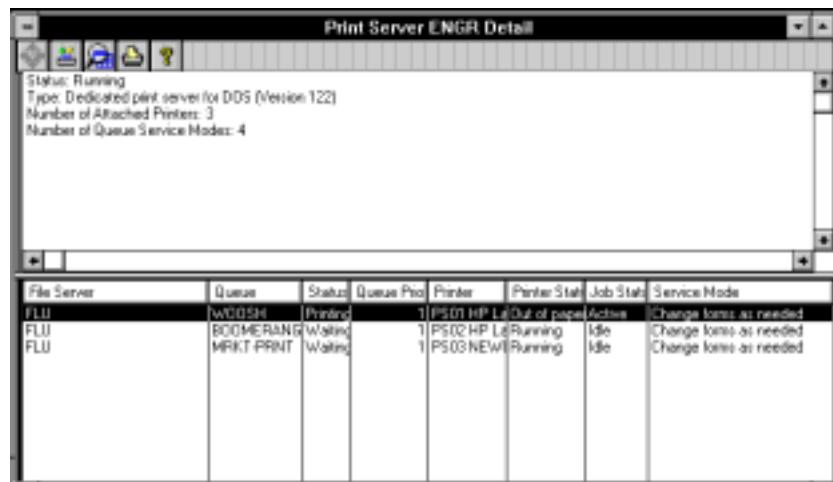
The Print Server Configuration window contains the following information about the print server, including which print queues it is servicing.

◆ **Status**—Describes whether the print server is running.

- **Type**—Describes whether the print server exists as a NetWare Loadable Module™ (NLM™) file on a NetWare server, as a dedicated print server for DOS, as a Value Added Process (VAP) on the file server, or as a VAP on a bridge. It also displays the version number.

- **Number of Attached Printers**—Number of printers attached to the machine that is running the print server.

- **Number of Queue Service Modes**—Number of service modes used by the print server.

For each print queue serviced by the selected print server, the information shown in Table 8-1 is available.

Table 8-1
Print Server Configuration Window Fields

Field	Explanation
Queue	Name of the print queue.
Status	Status of the print queue.
Queue Priority	Queue priority of the selected print queue.
Printer	Name of the printer attached to the print server designated to print the jobs from the print queue.
Printer Status	Operational state of the printer (running or not).
Job Status	Status indicating whether the print server is currently servicing any jobs from the selected print queue.
Service Mode	Mode indicating the priority of the factors used by the print server to determine which job gets printed next from the queues that the printer is servicing. The factors used are the queue priority, the job position in the queue, the form mounted on the printer, and the form required by the print job.

Monitoring File Servers

ManageWise provides current data about all the NetWare servers on which the NetWare Management Agent software is installed. It can provide the following information about the current NetWare server configuration data:

◆ System summary—Refer to "Monitoring a File Server's Configuration" on page 167

◆ CPU—Refer to "Monitoring CPU Speed and Utilization" on page 169

◆ NLM files—Refer to "Monitoring NLM Files" on page 170

◆ Memory use—Refer to "Monitoring Memory Usage" on page 172

◆ Network interfaces—Refer to "Monitoring Network Interfaces" on page 186

◆ Adapters—Refer to "Monitoring Adapters" on page 189

◆ Bound protocols—Refer to "Monitoring Bound Protocols" on page 191

◆ Disks—Refer to "Monitoring Server Hard Disk Information" on page 180

◆ Users—Refer to "Monitoring Users" on page 193

◆ Connections—Refer to "Monitoring Connections" on page 196

◆ Volumes—Refer to "Monitoring Volume Information" on page 175

◆ Queues—Refer to "Monitoring Queues" on page 183

◆ Open files—Refer to "Monitoring Open Files" on page 198

◆ Installed software—Refer to "Monitoring Installed Software" on page 199

Viewing File Servers

To view a list of file servers, select *View > All > NetWare File Servers.* The All NetWare File Servers window, shown in Figure 8-4, is displayed.

Note ▼ The list of file servers shown in the All NetWare File Servers window can either display only file servers in the database or display file servers in the database and file servers found dynamically. To set what is displayed, refer to *ManageWise 2.6 Setup Guide.*

Figure 8-4
All NetWare File Servers Window
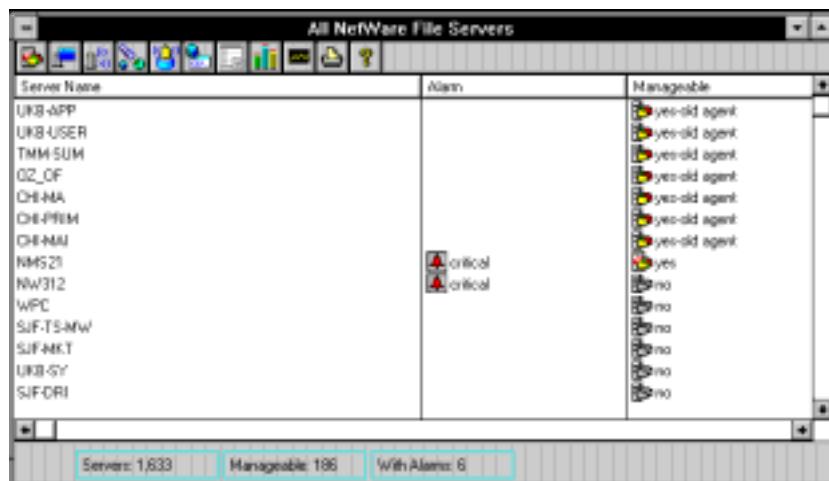
The status bar at the bottom of the window displays the total number of NetWare servers, the number of those servers that are manageable, and the number of manageable servers that have alarms.

Table 8-2 describes the All NetWare File Servers fields.

Table 8-2
All NetWare File Servers Fields

Field	Explanation
Server Name	Name of the file server.
Alarm	Displays the highest severity unacknowledged alarm received from this server. The alarm can be critical, major, or minor. Only file servers in the database show alarms. File servers discovered dynamically show an n/a in this field.

Table 8-2 *continued*
All NetWare File Servers Fields

Field	Explanation
Manageable	States whether the server is running NetWare Management Agent. A server must be running NetWare Management Agent to be manageable. Servers with 2.x version of NetWare Management Agent display a NetWare Management Agent icon and the word *Yes*. Servers with an older version (1.5 or 1.6) of NetWare Management Agent display a NetWare Management Agent icon and the words *Yes—old agent*. Servers that are not manageable display a grayed out NetWare Management Agent icon and the word *No*.

The file servers listed in the table can be sorted by fields. If you sort the table by the Server Name field, servers are listed alphabetically with server names beginning with numerals coming first.

If you sort the table by the Alarm field, servers are listed by severity. Servers are listed from most severe alarm to least severe. If servers have alarms with the same severity, they are listed alphabetically.

If you sort the table by the Manageable field, servers are listed by the version of NetWare Management Agent on the server. Servers with 2.6 version of NetWare Management Agent are listed first, servers with an old version of NetWare Management Agent are listed next, and servers that do not have NetWare Management Agent (unmanageable) are listed last. Servers with the same version of NetWare Management Agent are listed alphabetically.

To view a specific file server from the All NetWare File Servers window, do one of the following:

◆ Double-click a server.

◆ Select a specific server, and then press the File Server action bar button.

◆ Select a specific server, and then select *File > Open > File Server*.

If you use the menu command, a dialog box appears. You can specify the server by name, IP address, or IPX address.

Note ▼ You can also view a specific file server by double-clicking the target server icon when viewing an internetwork map, a segment map, or a custom map. Manageable servers appear on the map in color.

If the server you selected is not manageable, the Database Object Editor appears on the screen. You can use the Database Object Editor to record information about the server. Refer to "Using the Database Object Editor" on page 50 for more information about the Database Object Editor.

If the server you selected is running NetWare Management Agent 2.x, the server Configuration window appears on the screen and displays icons summarizing the selected server's configuration. The configuration summary is information obtained by the NetWare Management Agent software on the server. This window is the starting point for all current configuration data for NetWare file servers in which the NetWare Management Agent software is installed.

Note ▼ Other ManageWise components (such as the NetExplorer™ system) and third-party software might add icons to the Configuration window.

The Configuration window, shown in Figure 8-5, displays icons summarizing the selected server's configuration.

Figure 8-5
Configuration
Window

Monitoring a File Server's Configuration

A file server's configuration window displays general configuration information in the form of icons with related statistics, if any. For example, if a file server has one disk drive, a 1 appears under the disk

drive icon. ManageWise provides a summary of the server that you can view.

To display a configuration overview, follow these steps:

Procedure

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the System Summary icon, shown below, or select the System Summary icon and select** *File > Open > Selected Object***.**

System Summary

The System Summary detailed display window, shown in Figure 8-6, is displayed.

Figure 8-6
System Summary
Detailed Display
Window


```
                               SJF-ATHEN - System
       Server Name: SJF-ATHEN
       Internal Net#: 01055A66
       OS Description: Novell NetWare 4.10
       Release Date: 11/8/94
       Time Zone: PST8PDT
       Login State: enabled
       Language: English
   Maximum Connections: 250
              Name: CN=SJF-ATHEN.OU=MS.OU=eng.OU=nmp.O=novell
       Bindery Context: OU=MS.OU=ENG.OU=NMP.O=NOVELL
       Tree Name: SJF-NMP41
       Current Time: 1/12/95 7:19:16 AM
             Uptime: 0 days, 18 hours, 15 minutes
              CPUs: 1
               RAM: 15936
   Network Interfaces: 3
           Adapters: 2
             Disks: 2
```

Monitoring CPU Speed and Utilization

NetWare automatically determines the CPU speed of the server when it is loaded. Because CPU speed can be a major determinant of server performance, it is important to be able to determine the server speed for each server. ManageWise lets you see this information easily for all your managed servers.

CPU speed is useful for comparing a variety of hardware platforms to see their relative performance running NetWare. Differences in CPU speed must be taken into account when you compare server performance and loading between multiple servers.

For instance, one server might be handling twice as many users as another, but if the CPU is twice as fast, then the load might still be distributed correctly.

The CPU speed is determined by the following elements:

◆ CPU clock speed (20 MHz, 25 MHz, 33 MHz, and so on)

◆ CPU type (80386SX, 80386, 80486, and so on)

◆ Number of wait states (0, 1, 2, and so on)

An 80486 running at 33 MHz should get a rating of about 915. If your computer has a lower rating than you expected, check the CPU speed rating.

CPU utilization can be an important factor in the speed of the server. If the utilization of a server is consistently high, you might experience a slow server. A faster CPU might achieve better performance. For other possible causes of a slow server, refer to "Server Is Slow" on page 210.

To display the CPU speed and utilization data, follow these steps:
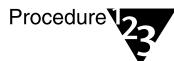
Procedure

1. View the file server's Configuration window.

Refer to "Viewing File Servers" on page 165 for instructions.

The target server's Configuration window is displayed.

2. Double-click the CPUs icon, shown below, or select the CPUs icon and select *File > Open > Selected Object*.
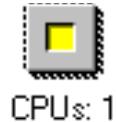
CPUs: 1

The number below the CPUs icon represents the number of CPUs discovered by NetWare Management Agent.

The CPUs window appears, which displays the following information:

◆ The server's workload, as a utilization percentage

◆ A description of the server's CPU, which lists its type, its computed speed rating, and the type of bus used

◆ Status information about each processor on the server

This information is useful if you want to obtain information about each processor in a Symmetric Multiprocessing (SMP) server. Any of the following status messages can appear in this column:

Unknown—The current state of the processor is unknown.

Warning—An unusual error condition was reported by the operational software on the server, but the processor is still operational.

Running—The processor is running and no error conditions are known. A non-SMP server typically shows this status.

Testing—The processor is not available for use because it is in a testing state.

Down—The processor is not available for any use.

Monitoring NLM Files

You can determine which NLM files are currently loaded on the server, the NLM files' versions and release dates, and the memory used by each NLM file.

To view NLM files on a server, follow these steps:

Procedure 23

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the NLMs icon, shown below, or select the NLMs icon and select *File > Open > Selected Object*.**

   The NLMs detailed display window, shown in Figure 8-7, is displayed.

Figure 8-7
NLMs Detailed
Display Window

The status bar at the bottom of the window displays the total number of NLM files on the server and the combined code and memory size, in kilobytes, used by the NLM files.

The NLMs detailed display window contains the current information about the server NLM files, shown in Table 8-3.

Table 8-3
NLM Table Fields

Field	Explanation
NLM Name	Name of the NLM.
Version	Current version of the NLM.
Released	Date and time the NLM was released.
Memory (Bytes)	Sum of data size, code size, and allocated memory (short term, semipermanent, and non-movable cache) for the NLM file.
Description	Description of the NLM.
Copyright	Copyright information for the NLM.

For more information about how to manipulate this table (resize columns, move columns, sort data, and so on), refer to *ManageWise 2.6 Setup Guide*. Data in the table can be printed or exported for use in other programs (a spreadsheet program, for example). You can find print and export information in *ManageWise 2.6 Setup Guide*.

Monitoring Memory Usage

Memory usage can be displayed as a two-dimensional or three-dimensional pie chart, and the values can be displayed as either percentages or absolute values.

Correct memory allocation is essential to achieving optimum performance on NetWare servers. The biggest factor affecting a server's performance is having enough memory for file caching. Loading NLM files and running applications takes memory away from cache buffers, possibly slowing the server (refer to "Server Is Slow" on page 210). By monitoring two memory usage trends, average percentage of Dirty Cache Buffers and percentage of Cache Buffers, you can determine whether the amount of memory you allocate is enough to keep your server from slowing. Refer to "Viewing Trends" on page 212, "Monitoring Cache Buffers" on page 209, and "Monitoring Dirty Cache Buffers" on page 209 for more information about monitoring trends.

To increase the size of the cache buffer, you can unload unnecessary NLM files, unload applications, allocate more memory to the cache buffers (refer to "SET Server Parameters" on page 220), install more RAM in the server, or a combination of these actions.

To display current RAM allocation, follow these steps:

Procedure 23

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the RAM icon, shown below, or select the RAM icon and select *File > Open > Selected Object*.**

15936 KBytes

The text beneath the icon shows the amount of RAM installed on the selected server in kilobytes.

The Memory Usage detailed display window, shown in Figure 8-8, is displayed. The chart, shown within the detailed display window, is updated dynamically every minute to show the current memory usage of the selected server. You can change the frequency of the update by changing the polling period in the Global Preferences (refer to *ManageWise 2.6 Setup Guide*).

At the side of the window are buttons that control the following features:

◆ **Absolute value**—Displays memory allocation using absolute values.

◆ **Percentage**—Displays memory allocation using percentages.

◆ **Two-dimension**—Displays the pie chart as a two-dimensional figure.

◆ **Three-dimension**—Displays the pie chart as a three-dimensional figure.

◆ **Rotate View**—Rotates the view of the pie chart.

A legend listing the pie chart categories appears at the bottom of the detailed display window.

Figure 8-8
Memory Usage Detailed Display Window
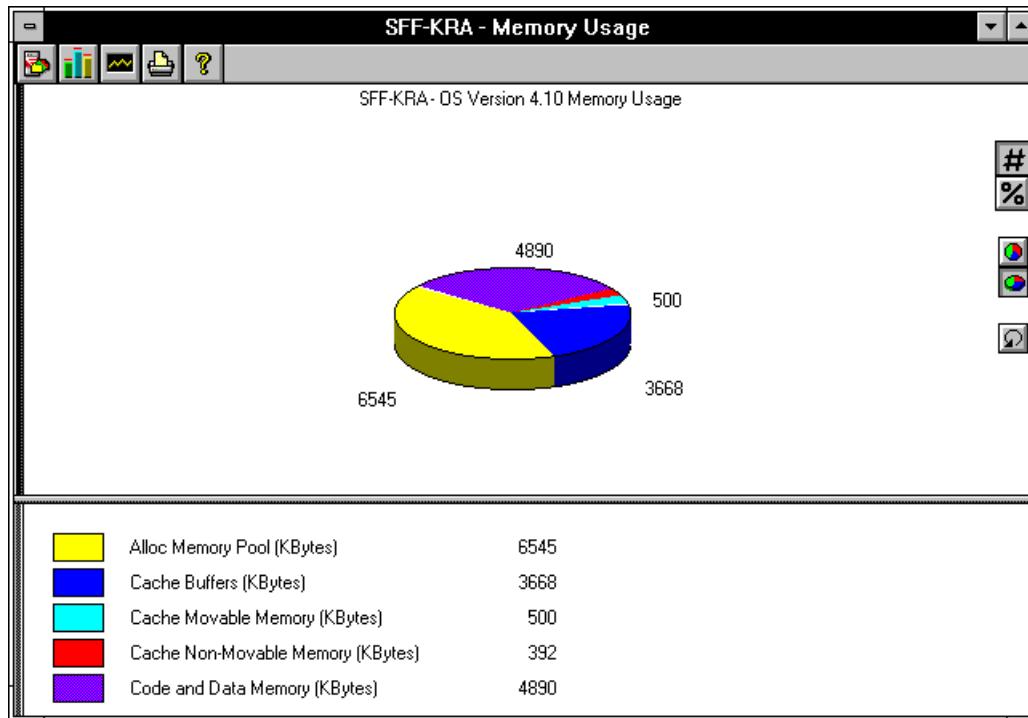
The Memory Usage detailed display window shows the following data:

◆ **Alloc Memory Pool** (KBytes)—Allocates memory to NLM files for temporary or short-term use. After memory is allocated to this pool, it is not returned to the regular cache buffers. When the module is unloaded, the allocated memory returns to the pool for other NLM files.

◆ **Cache Buffers** (KBytes)—Displays the number of kilobytes used for file cache buffers. File caching allows faster access to frequently used files by holding the file in memory. If the server is slow, the file cache might not be large enough.

◆ **Cache Movable Memory** (KBytes)—Displays the number of kilobytes stored in the movable file cache buffers. When a program is no longer using these buffers, it returns the buffers to the cache buffer pool.

◆ **Cache Non-Movable Memory** (KBytes)—Displays the number of kilobytes stored in the fixed file cache.

◆ **Code and Data Memory** (KBytes) (NetWare 4™ only)—Displays the number of kilobytes taken by the code and data segments of all NLM files and SERVER.NLM. (NetWare 3.11 allocated the NLM code and data segments from the cache non-movable memory pool.)

◆ **Permanent Memory Pool** (KBytes) (NetWare 3.11 and 3.12 only)—Contains both permanent and semipermanent memory pools. Both pools are used for long-term memory needs such as directory cache buffers and packet receive buffers. After this memory is allocated as either permanent or semipermanent, the memory is not returned to the regular cache buffers unless the server is restarted.

Monitoring Volume Information

NetWare server disk storage space is divided into volumes. ManageWise enables you to view various data about the volumes in a server running NetWare Management Agent software, such as size, free space, how the volumes are distributed across the disks, and which users are using the space.

ManageWise lets you check the exact amount of space available on every volume in the server. ManageWise also generates an alarm when free space on a volume drops below a set threshold (refer to "Monitoring Free Space on a Volume" on page 204 and "Monitoring Volume Usage" on page 208). If you save these alarms to the database, you can check the Alarm Report to get more information about the server and the volume.

If only some of the volumes are filling up, you can allow users to use the emptier ones or rearrange the volumes or add hard disk space. By presenting this information in one unified table, you can avoid the process of checking each volume individually to determine how much space is available.

You can also keep track of which volumes are fault tolerant, which volumes are on which physical disk, and so on. This type of information is invaluable whenever there is a disk-related problem, whether it is as easy to handle as a volume filling up or something as potentially catastrophic as a hard disk crash.

To display volume information, follow these steps:

Procedure

1. **View the file server's Configuration window.**

    Refer to "Viewing File Servers" on page 165 for instructions.

    The target server's Configuration window is displayed.

2. **Double-click the Volumes icon, shown below, or select the Volumes icon and select *File > Open > Selected Object*.**

Volumes: 2

The Volumes detailed display window, shown in Figure 8-9, is displayed.

Figure 8-9
**Volumes Detailed
Display Window**

This window displays three tables. The top table, called the Volume Configuration table, displays information about all the volumes in the server. The middle table, called the Volume Segment table, displays details about the segments of the selected volume. The bottom table, called the Volume Usage table, lists user disk usage for the selected volume.

Note ▼ You can select a different volume by clicking on the volume in the upper table.

If you select a CD-ROM volume, no segment information is available because CD-ROM volumes do not have any segments.

The status bar at the bottom of the window displays the total number of volumes on the server, the selected volume, the number of segments on the selected volume, and the number of users on the selected volume.

Volume Configuration Table

> The Volume Configuration table includes the information shown in Table 8-4 for each volume, on separate rows.

Table 8-4
Volume Configuration Table Fields

Field	Explanation
Volume Name	Name of the volume. This is not a directory services name.
Size (MB)	Size of the volume in megabytes.
Free (MB)	Free space on the volume in megabytes. As files are added or expanded, this number approaches zero. A pie chart shows you how much of the total volume size is free.
Used (MB)	Number of megabytes currently in use. As files are added or expanded, this number approaches that shown in the size column. A pie chart shows you how much of the total volume size is used.
Status	Whether the volume is mounted. If the volume is not mounted, only the volume name is listed.
Name Spaces	Name spaces that are supported on the volume. Name spaces supported are DOS, Macintosh*, NFS*, FTAM, OS/2*, and NT.
Attributes	Attributes of the volume. Attributes a volume can have are block suballocation, file compression, data migration, auditing, and read-only. A volume can have a combination of attributes, such as a read-only volume with block suballocation enabled.
# Disks	Number of disks that the given volume spans.
DS Name	Directory service name of the volume.
Purgeable KB	Amount of space that can be freed by purging the deleted files whose purge date has expired.
Non-purgeable KB	Amount of space taken by the deleted files whose purge dates have not yet expired.
Block Size KB	Block size on the volume in kilobytes.
Dir Slots	Number of directory slots on the volume.
Used Dir Slots	Number of directory slots in use.

Field	Explanation
File System Name	Listed only if the volume is remote and the file system name is the remote mount point; for example, SITE1:/usr/x.

Note ▼ Double-click a volume to view information specific to that volume. The information you view is limited to the information shown in the Volume Configuration table of the Volume detailed display window.

Volume Segment Table

The Volume Segment table in the Volumes window includes the information shown in Table 8-5 about the segments of the selected volume.

Table 8-5
Volume Segment Table Fields

Field	Explanation
ID	Number assigned to the segment for identification.
Logical Partition ID	Number assigned to a logical partition for identification.
Physical Partition ID	Number assigned to a physical partition for identification.
Size (MB)	Size of the segment in megabytes.
Fault Tolerance	Type of fault tolerance used. Types that can be used are duplex and mirrored. If there is no fault tolerance, the word *None* is shown.
Disk Drive	Name of the disk drive on which the segment resides.

Note ▼ Double-click a segment to view information specific to that segment. The information you view is limited to the information shown in the Volume Segment table of the Volume detailed display window.

Volume Usage Table

The Volume Usage table in the Volumes window includes the information shown in Table 8-6 about the users of the selected volume.

Table 8-6
Volume Usage Table Fields

Field	Explanation
Used KB	Number of kilobytes currently in use.
Limit KB	Number of kilobytes to which the user is limited.
User Name	User's login name.

Note   Double-click a username to view information specific to that user. The information you view is limited to the information shown in the Volume Usage table of the Volume detailed display window.

Monitoring Server Hard Disk Information

Disk drives are the primary storage devices for NetWare servers. ManageWise enables you to get detailed information about the disk drives in a managed server, including disk size in megabytes, disk types, block size, and so on. You can also view partition information for each disk drive. Partition information is especially informative because you can determine whether a partition is fault tolerant and whether the hard disk is losing data integrity.

Fault tolerance of a partition is part of the detailed information provided by ManageWise. To determine whether a hard disk is losing data integrity, examine the redirected area. A number in the redirected area indicates the number of data blocks that have been redirected to the Hot Fix™ Redirection Area to maintain data integrity. The higher the redirected area number, the more faulty blocks there are on the hard disk. A redirected area growing over a period of time indicates a hard disk going bad.

For information about the Hot Fix Redirection Area, refer to *Concepts* in your NetWare server documentation. For information about collecting and viewing trend data, refer to "Setting Trends and Thresholds" on page 216 and "Viewing Trends" on page 212.

To display disk drive information, follow these steps:

Procedure 23

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Disks icon, shown below, or select the Disks icon and select *File > Open > Selected Object*.**

Disks: 2

   The Disks detailed display window, shown in Figure 8-10, is displayed. It displays two tables of information about the selected disk: configuration and physical partitions.

Figure 8-10
Disks Detailed Display Window

SJF-ATHEN - Disks								
Disk Name	Size MB	Access	Status	Type	Driver Descr	Block Size	Heads	Cylinders
Device # 0 ISA Type 098 (20000000)	202	Read/Write	Operational	Hard Disk	NetWare 4.01	16,384	16	682
Device # 1 ISA Type 098 (20000100)	202	Read/Write	Operational	Hard Disk	NetWare 4.01	16,384	16	682

Device # 0 ISA Type 098 (20000000) - Partitions

Logic	Physi	Type	Size MB	Redirection Area KB	Redirected Area K	Reserved Area	Fault Tolerance
0	0	DOS (12-bit FAT) Partition	10	0	0	0	None
1	1	NetWare Partition #1	192	2,236	0	96	None

| Disks: 2 | Device # 0 ISA Type 098 (20000000) | Partitions: 2 |

The status bar at the bottom of the window displays the total number of disks in the server, the name of the selected disk, and the number of partitions on the selected disk.

Disks Configuration Table

The Disks Configuration table contains the information shown in Table 8-7.

Table 8-7
Disks Configuration Table Fields

Field	Explanation
Disk Name	Name of the disk drive.
Size MB	Total size in megabytes.
Access	Whether the disk drive is readable and writable or just readable.
Status	Whether the disk is operational.
Type	Type of media. Media types can include hard disk, floppy disk, tape, optical disk (read-only, write once read many, and read/write), or RAM disk. If unidentifiable, *other* or *unknown* is listed in this field.
Driver Description	Name of the driver used by the disk drive.
Block Size (Bytes)	Number of blocks used on the disk, in kilobytes.
Heads	Number of read/write heads on the disk drive.
Cylinders	Number of cylinders on the disk drive.
Sectors/Track	Number of sectors per track on the disk drive.
SCSI Target Address	Target address for SCSI controllers or the unit number for other devices.
SCSI LUN	Logical unit number for SCSI devices or the value zero for other devices.

Note ▼ Double-click a disk to view information specific to that disk. The information you view is limited to the information shown in the top table of the Disks detailed display window.

Disks Physical Partitions Table

The Disks Physical Partitions table includes the information shown in Table 8-8 about all the physical partitions in a given disk.

Table 8-8
Disks Physical Partitions Table Fields

Field	Explanation
Logical Partition ID	Number assigned to a logical partition for identification.
Physical Partition ID	Number assigned to a physical partition for identification.
Type	Type of partition, including DOS, NetWare, and UNIX partitions.
Size MB	Size of the partition, in megabytes.
Redirection Area KB	Size of the entire Hot Fix Redirection Area.
Redirected Area KB	Number of bad blocks Hot Fix found.
Reserved Area KB	Number of Hot Fix redirection blocks reserved for system use.
Fault Tolerance	Type of fault tolerance used. Types that can be used are duplex and mirrored. If there is no fault tolerance, the word *None* is shown.

Note ▼ Double-click a partition to view information specific to that partition. The information you view is limited to the information shown in the bottom table of the Disks detailed display window.

If you selected a CD-ROM in the Disks Configuration table, no partition information is available because CD-ROM disks do not have any partitions.

Monitoring Queues

The Queues object group lists queues, jobs in the queues, and servers attached to the queues. By monitoring the Queues object group, you can see whether a queue is busy or stalled. If the queue is a print queue, you can determine whether the printer is down or whether print jobs take time to print because of the size of the queue or the size of jobs in the queue.

To monitor NetWare print queues, follow these steps:

Procedure ▼

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Queues icon, shown below, or select the Queues icon and select *File > Open > Selected Object*.**

Queues: 2

The Queues detailed display window, shown in Figure 8-11, is displayed.

**Figure 8-11
Queue Detailed
Display Window**

This window displays three tables. The top table lists information about all the queues on the server. The middle table lists all the jobs in the selected queue. The bottom table lists all print servers attached to the selected queue.

The status bar at the bottom of the Queues detailed display window displays the number of queues, the queue currently selected, the number of jobs in that queue, and the number of print servers attached to that queue.

Queues Configuration Table

The Queues Configuration table (top table) lists the information shown in Table 8-9 for every queue, on separate rows for each queue.

Table 8-9
Queues Configuration Table Fields

Field	Explanation
Queue Name	Name of the queue on the server.
Type	Type of queue. The queue can be designated a job queue, archive queue, print queue, or other.
# Jobs	Number of job entries in the queue.
# Print Servers	Number of print servers assigned to a queue.
Volume	Name of the volume where the directory created for this queue resides.
Add Job State	Indicates whether more jobs can be added to the queue.
Attach State	Indicates whether queue servers can attach to the queue.

Queues Jobs Table

The Queues Jobs table (middle table) in the Queues detailed display window includes the information shown in Table 8-10 about the jobs in the selected queue.

Table 8-10
Queues Jobs Table Fields

Field	Explanation
Job #	Number assigned to the job in the queue.
Position	Priority of the job in the queue.
Bytes	Size, in bytes, of the job in the queue.
Description	Description of the job in the queue.

Table 8-10 *continued*
Queues Jobs Table Fields

Field	Explanation
User	Login name of the user submitting the job.
Entry Time	Time the job entered the queue.
Control Flags	Job control flags that are set. Job control flags that can be set are Service Auto-Start, Execute, Entry Open, User Hold, and Operator Hold.
Target Time	When the job is to finish.
Target Server	Server the queue is supposed to use. The job might go to another server if the target server is overloaded.
Actual Server	Server currently processing the job. If the job is currently not being handled, this field is empty.

Attached Servers Table

The Attached Servers table (bottom table) in the Queues detailed display window includes the information shown in Table 8-11 about the print servers attached to the selected queue.

Table 8-11
Attached Servers Table Fields

Field	Explanation
Status	Status of the queue server. A server's status can be active, inactive, or unknown.
Name	Name of the print server servicing the queue.

Monitoring Network Interfaces

Network interfaces are interfaces used by your server's network boards (adapters). Network interfaces define the network protocol and frame type used by the network to which a network board is attached. For each network board in a server, the Network Interfaces detailed display shows interface information. One network board can have a number of different network protocols bound to it (an IP and IPX protocol, for example).

You can use the Network Interfaces detailed display to help you when adding network interfaces to other network boards or as a troubleshooting tool. When adding network interfaces to other network boards, compare the frame type and protocol you want to use to an existing network board's frame type and protocol listed in the detailed display. By comparing frame types and protocols, you can avoid binding a frame type to an unsupported protocol.

Occasionally, a user cannot log in to a server because the frame type used by that person's system is different from the frame type used by the server. As a troubleshooting tool, you can use the Network Interfaces detailed display to determine why a user cannot log in to a server. Compare the user's frame type to the one used by the server. If they are different, you can change the frame type in the user's NET.CFG file, edit the user's frame type to match the server's frame type (refer to "Editing Adapter Information" on page 55), and restart the user's system.

To display network interface configuration data, follow these steps:

Procedure **23**

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Network Interfaces icon, shown below, or select the Network Interfaces icon and select *File > Open > Selected Object*.**

Network Interfaces: 3

   The Network Interfaces detailed display window, shown in Figure 8-12, is displayed.

Figure 8-12
Network Interfaces
Detailed Display
Window

The status bar at the bottom of the window displays the total number of network interfaces used by the server.

The Network Interfaces detailed display window contains the configuration information shown in Table 8-12.

Table 8-12
Network Interfaces Table Fields

Field	Explanation
Frame Type	Type of frame structure used by the server. NetWare supports four frame structures: Ethernet_802.3, Ethernet_II, Ethernet_802.2, and Ethernet_SNAP.
MAC Address	Media-access control address.
Description	Type of network board (Ethernet, token ring, FDDI).
Protocols	Protocol bound to the given frame type. The IP and IPX protocols are examples.
Line Speed	Current bandwidth, in bits/second, of the network board.
Type	Type of network interface, distinguished according to the physical link type and protocols; for example, Ethernet, token ring, or FDDI.
Logical Board #	Number assigned to the interface for identification.
Logical Board Name	Name assigned to the board for identification.

Monitoring Adapters

A common problem is a server's inability to perform a task due to adapter configuration problems. Duplicate I/O port addresses or duplicate interrupts are problems you might encounter. Using ManageWise, you can quickly determine I/O port address or interrupt conflicts by viewing the list of adapters.

Note ▼ ManageWise does not monitor only network boards. Disk storage controller boards, CD-ROM controller boards, and network boards are a few of the adapters that might be monitored.

To monitor the adapters attached to managed servers, follow these steps:

Procedure ▼ **1. View the file server's Configuration window.**

Refer to "Viewing File Servers" on page 165 for instructions.

The target server's Configuration window is displayed.

2. Double-click the Adapters icon, shown below, or select the Adapters icon and select *File > Open > Selected Object*.

Adapters: 2

The Adapters detailed display window, shown in Figure 8-13, is displayed. The number under the icon indicates the number of adapters in the server.

Figure 8-13
Adapters Detailed
Display Window

The status bar at the bottom of the window displays the total number of adapters in the server.

Table 8-13 describes the Adapters Configuration table fields.

Table 8-13
Adapter Configuration Table Fields

Field	Explanation
Description	Description of the hardware for this adapter. Information provided in this field can include manufacturer, model, and version, or for network boards, a short board name and the board's burned-in MAC address.
Type	Type of adapter (network board, disk storage, and so on).
Devices Attached	Number of devices associated with an adapter. For example, the number of drives attached to a disk controller.
Driver Description	Description of the driver for this adapter.
Version	Version number of the driver software.
Interrupt Number	Unique interrupt number used by the adapter.
I/O Port	Unique I/O port block used by the adapter.
Memory	Unique memory address space used by the adapter.
DMA	Direct Memory Access channel used by the adapter.

Table 8-13 *continued*
Adapter Configuration Table Fields

Field	Explanation
Slot	Slot in which the adapter is installed (for adapters running on PS/2* or EISA machines).

Monitoring Bound Protocols

The Bound Protocols object group lists all the protocols bound to each network board in a server. Also listed are the number of packets sent and received over each protocol. By viewing the Bound Protocols object group, you can see which protocols have the most traffic.

To monitor bound protocols, follow these steps:
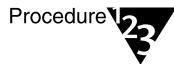
Procedure 23

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Bound Protocols icon, shown below, or select the Bound Protocols icon and select *File > Open > Selected Object*.**

Bound Protocols

The Bound Protocols detailed display window, shown in Figure 8-14, is displayed.

The status bar at the bottom of the window displays the total number of protocols bound to the server.

Table 8-14 describes the Bound Protocols table fields.

Table 8-14
Bound Protocols Table Fields

Field	Explanation
Protocol	Name of the protocol bound to the server.
Logical Board #	Number given to the board with this protocol to identify the board.
Logical Board Name	Name given to the board with this protocol to identify the board.
Address	Network address of the board using this protocol.
Pkts In	Number of packets received from the time the Bound Protocols detailed display window was opened.
Pkts Out	Number of packets sent from the time the Bound Protocols detailed display window was opened.
Description	Full name of the protocol.

Monitoring Users

Monitoring users is most helpful when you want to back up a server's hard disk or shut down a server. By viewing users first, you can determine whether users are busy. If users are busy, indicated by read and write activity, you can postpone server maintenance until a time when there is little or no user activity.

Monitoring users is also useful as a security aid. If a user account has a large number of bad login attempts, an unauthorized user might be trying to log in to the server from that account.

To monitor users of managed servers, follow these steps:

Procedure 23

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Users icon, shown below, or select the Users icon and select *File > Open > Selected Object*.**

Users: 2

The Users detailed display window, shown in Figure 8-15, is displayed.

Figure 8-15
Users Detailed
Display Window

The window displays two tables. The top table (Logged-in Users) lists all the current users logged in to the server. The bottom table (User Accounts) lists all the existing user accounts on the server. The status bar at the bottom of the window displays the total number of user accounts on the server and the number of users logged in to the server.

Note　The Users window displays the Logged-In Users and User Accounts tables for NetWare 3™ servers and NetWare 4 servers whose bindery context is defined. For NetWare 4 servers whose bindery context is undefined, the Users window displays only the Logged-in Users table.

Table 8-15 describes the Logged-in Users table fields.

Table 8-15
Logged-in Users Table Fields

Field	Explanation
Login Name	User's login name.
Connection #	Number of the connection used by the client.
Privilege	User's rights that determine what operations can be performed on files, directories, or objects.

Field	Explanation
Status	Whether the user is logged in.
Client Address	Address of the user's workstation.
Login Time	Day and time that the user logged in to the server.
Open Files	Number of files the user has open.
Locked Records	Number of locked records the user has open.
Read KB	Kilobytes of data read since the Users detailed display window was opened.
Written KB	Kilobytes of data written since the Users detailed display window was opened.
NCP Requests	Number of NetWare Core Protocol™ (NCP™) requests made since the Users detailed display window was opened.

Table 8-16 describes the User Accounts table fields.

Table 8-16
User Accounts Table Fields

Field	Explanation
Login Name	User's login name.
Disk Usage KB	Amount of disk space used by each account across all volumes on the server.
Account Status	Whether the account is valid, invalid, or expired.
Password Status	Whether the password is valid, invalid, or expired.
Last Login	Last time the user logged in to this server.
Real Name	Full name of the user.
Bad Login Attempts	Number of times the user attempted to log in with a bad password since the server started.
Bad Login Address	Network address of the workstation from which the last bad login attempt was made.

Monitoring Connections

The Connections object group is similar in scope to the Users object group. Both monitor the status of users and user connections. The difference is that the Connections object group emphasizes connection data and the Users object group emphasizes user data. Monitoring connections is useful in determining whether the server is busy and, if so, in determining which connections are the busiest.

To monitor user connections of managed servers, follow these steps:

Procedure

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Connections icon, shown below, or select the Connections icon and select _File > Open > Selected Object_.**

Connections: 12

The Connections detailed display window, shown in Figure 8-16, is displayed.

Figure 8-16
Connections
Detailed Display
Window

Table 8-17 describes the Connections table fields.

Table 8-17
Connections Table Fields

Field	Explanation
Connection #	Number of the connection used by the client. Connection 0 is used by the system.
Connection Owner	User's login name.
Privilege	Connection login privileges. A connection's privileges can be one or a combination of the following: SUPERVISOR, OPERATOR, AUDITOR, high privilege, second authentication, second high privilege, or unknown.
Status	Login status of the user. The status can be one or a combination of the following: Not logged in, logged in, need security change, MacStation, connection abort, audited, authenticated temporary, audit connection recorded, DS audit connection recorded, and logout in progress.
Client Address	Transport address of the connection.
Connected	Day and time of the established connection.
Open Files	Number of files currently opened by the connection.

Table 8-17 *continued*
Connections Table Fields

Field	Explanation
Locked Records	Number of file records currently locked by the connection.
Read KB	Number, in kilobytes, of data read since the Connections detailed display window was opened.
Written KB	Number, in kilobytes, of data written since the Connections detailed display window was opened.
NCP Requests	Number of NCP requests made since the Connections detailed display window was opened.

Monitoring Open Files

When you view the Open Files object group, you see what files are currently open, what volume they are on, who opened a particular file, and which connection is used. Viewing open files is useful when you plan on backing up the system. Files that are open cannot be backed up. By first seeing what files are open, you can notify users with open files that a backup is imminent.

To monitor open files, follow these steps:

Procedure

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Double-click the Open Files icon, shown below, or select the Open Files icon and select *File > Open > Selected Object*.**

Open Files: 11

The Open Files detailed display window, shown in Figure 8-17, is displayed.

Figure 8-17
Open Files Detailed
Display Window

Table 8-18 describes the Open Files table fields.

Table 8-18
Open Files Table Fields

Field	Explanation
Connection #	Number of the connection that opened the file.
User	Name of the user who opened the file.
Volume	Volume in which the open file resides.
File	Name of the open file, including the directory path.

Monitoring Installed Software

The Installed Software object group shows you products that were installed on the server in addition to NetWare. Only software installed using the NetWare PINSTALL utility is listed. By viewing the Installed Software object group, you know more about the server's configuration.

To view installed software, follow these steps:

1. View the file server's Configuration window.

Refer to "Viewing File Servers" on page 165 for instructions.

The target server's Configuration window is displayed.

2. Double-click the Installed Software icon, shown below, or select the Installed Software icon and select *File > Open > Selected Object*.

Installed Software

The Installed Software detailed display window, shown in Figure 8-18, is displayed.

Figure 8-18
Installed Software
Detailed Display
Window

Software installed using the NetWare install utility is listed in the detailed display. Listed beside each program is that program's version number and functional description.

Monitoring NetWare SFT III Servers

If you have a NetWare SFT III™ server on your network, the ManageWise Console software lists the MSEngine and two IOEngines in the View All Servers window. You open any engine's configuration window as you do any NetWare server (refer to "Viewing File Servers" on page 165).

The MSEngine's Configuration window shows three SFT III icons in addition to the configuration icons previously described in this chapter. Of these three SFT III icons, one represents the MSEngine and the remaining two represent the IOEngines. Information displayed for some SFT III server configuration icons differ from information displayed for their NetWare server counterparts. The differences are as follows:

- ◆ **System Summary**—Gives information about the MSEngine, which differs from that for the IOEngines.

- ◆ **CPU**—Shows the MSEngine Virtual Processor as the CPU.

- ◆ **NLM**—Shows the NLM files running. Some NLM files, such as ISADISK.NLM and other NLM files that allow hardware access, run only on the IOEngines.

- ◆ **Memory Allocation**—Gives the allocation for the MSEngine only.

- ◆ **Network Interfaces**—The frame type for interfaces on the MSEngine is VIRTUAL_LAN.

- ◆ **Adapters**—Shows the IOEngines as adapters.

- ◆ **Bound Protocols**—Includes the File Server Virtual IPX driver.

Information displayed for disks, users, connections, volumes, queues, open files, and installed software, the other SFT III server configuration icons in the configuration window, is similar to that given for NetWare server configuration icons.

You can view one of the IOEngine Configuration windows in three ways:

- ◆ Open the IOEngine directly by selecting *File > Open > NetWare Server* and entering the IOEngine address.

◆ Double-click one of the IOEngine icons in the View All Servers window.

◆ Double-click one of the IOEngine icons in the MSEngine configuration window.

The IOEngine Configuration window displays the icons for the MSEngine, this IOEngine (grayed out), and the other IOEngine, along with the following icons:

◆ **System Summary**—Gives information about the IOEngine. This information differs from that given for the MSEngine.

◆ **NLM**—Shows the NLM files running. Some NLM files, such as the directory services NLM files, run only on the MSEngine, while hardware-specific NLM files, like ISADISK.NLM, run only on the IOEngine.

◆ **Memory Usage**—Shows allocation among DOS memory, MSEngine memory, IOEngine memory, and Unclaimed memory. The MSEngine memory amount should be the same as the total memory shown for the MSEngine memory allocation.

◆ **Network Interfaces**—Network interfaces for an IOEngine include both VIRTUAL_LAN and a standard frame type (such as ETHERNET_802.2).

◆ **Adapters**—Adapters include the network boards and Mirrored Server Link™ (MSL™) boards. The MSL boards connect the SFT III primary and secondary servers.

◆ **Bound Protocols**—Includes the IOEngine Virtual IPX Driver.

◆ **MSL**—Shows the following statistics for the MSL board:

  ◆ **Description**—MSL board type.

  ◆ **State**—Whether the board is active or inactive. If you have multiple MSL boards, only one is active at a time.

  ◆ **Speed**—Speed of transmission in megabits per second.

  ◆ **Sends**—Number of packets the board sent since you opened the MSL detailed display window.

  ◆ **Receives**—Number of packets the board received since you opened the MSL detailed display window.

- ◆ **In Errors**—Number of errors in packets received since you opened the MSL detailed display window.

- ◆ **Out Errors**—Number of errors in packets sent since you opened the MSL detailed display window.

Monitoring Additional Network Services

In addition to the basic file, print, and routing services, a NetWare server can provide a number of optional and useful network services. For example, it can act as one or more of the following:

- ◆ Communication server

- ◆ Apple* file server

- ◆ NFS server

- ◆ FTAM file server

- ◆ Hub

- ◆ NetWare LANalyzer® Agent™ software, a remote network monitor (RMON) agent

ManageWise contains a NetWare utility that enables you to get information about the existence of these network services on a NetWare server.

To display this information, follow these steps:
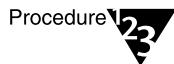
Procedure 23

1. **View the file server's Configuration window.**

   Refer to "Viewing File Servers" on page 165 for instructions.

   The target server's Configuration window is displayed.

2. **Check for icons that identify these services.**

In addition to gathering server information, ManageWise can gather detailed information about NetWare routers, NetWare hubs, and NetWare LANalyzer Agent servers. For more information, refer to the other manuals in the ManageWise set.

Monitoring Trends

ManageWise automatically collects statistics about a manageable server's configuration. ManageWise collects statistics concerning the server's CPU utilization, the number of packets transmitted or received by the server, the free space left in a volume, and so on. Monitoring trends can be both a planning tool and a troubleshooting tool.

Monitoring Trends as a Planning Tool

You can monitor trends over a long period of time and use this data as a planning tool. Some examples of using trend data as a planning tool are as follows:

◆ Monitoring Free Space on a Volume

◆ Monitoring Print Queues

◆ Monitoring the Number of Users on NetWare 3 Servers

By monitoring a trend, you can estimate when to take preventive action (such as increasing volume free space, moving users to other print queues, and moving users to other servers for the previously listed examples).

Monitoring Free Space on a Volume

You can monitor the free space left in a volume and estimate when the volume will be full. With this estimation, and continued monitoring, you can plan when to purchase additional hard disks. To plan when to purchase an additional hard disk for the monitored server, follow these steps:

Procedure

1. **View the longest Free Space on Volume trend possible.**

   Refer to "Viewing Trends" on page 212.

   View the longest trend possible because the more data you accumulate, the more accurate your estimation. The longest historical trend you can view depends on the amount of trend data previously collected. For example, if you started collecting trend data a week ago, you can view historical trends spanning one hour, one day, one week, or one month. The hourly or daily view might

show too much detail, whereas the monthly view might show too little detail. The weekly view is the logical choice because the trend graph is complete without showing too much detail (remember that this trend is for planning purposes; therefore, you do not need to view short-term events).

2. **Extrapolate from the graph when you believe volume usage will reach a point where you must add disk space.**

   Determine the point at which you must add disk space.

3. **Refine your estimate by viewing a long-term trend from time to time.**

Monitoring Print Queues

By monitoring the size and number of jobs in a print queue, you can decide whether you need another printer or whether you need to move users to another print queue. Typically, a job sent to a printer does not take long to print. Occasionally, a job sent to a printer takes longer to print because there is a large job in front of it in the print queue or there are a number of jobs in front of it in the print queue.

You should add a printer or move users to another print queue if it frequently takes a long time to print because either the majority of the jobs in the queue are large or there are too many users for the print queue.

To plan when to add a printer or move users to another print queue, follow these steps:

Procedure ▽
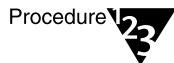
1. **Determine the maximum average size of a print job and the maximum number of print jobs you want for the print queue.**

   The values you choose are based on your experiences of when the size of jobs or the number of jobs in the print queue begins to affect the overall print time of a job.

2. **View the longest Ready Jobs in Queue (avg. #) and Ready Jobs in Queue (avg. KB) trends possible.**

   Refer to "Setting Trends and Thresholds" on page 216.

3. **Extrapolate from the graph when you believe the values you determined in Step 1 will be met.**

   This is your estimate.

4. **Refine your estimate by viewing long-term trends from time to time.**

Monitoring the Number of Users on NetWare 3 Servers

By monitoring the number of users, you can estimate when you will exceed the number of users for which your server is licensed. With this estimate, you can plan how to distribute users in the future—whether you will move users to other servers to stay under the licensing agreement or upgrade to a license allowing more users.

To plan when to move users or upgrade your license, follow these steps:

Procedure

1. **Determine the maximum number of users for the server.**

   Do this by double-clicking the System Summary icon in the server's Configuration window and viewing the value for Maximum Connections (refer to "Monitoring a File Server's Configuration" on page 167).

2. **View the longest Average Number of Logged-In Users trend possible.**

   Refer to "Setting Trends and Thresholds" on page 216.

3. **Extrapolate from the graph when you believe the number of users will reach a point where you must upgrade your license or move users to other servers.**

   Determine the point at which you must upgrade your license or move users. If you want, you can use the default threshold value for the average number of logged-in users. This value is set to 90 percent of the total number of users.

4. **Refine your estimate by viewing a long-term trend from time to time.**

Monitoring Trends as a Troubleshooting Tool

In addition to collecting trend statistics, you can set alarm thresholds. The alarm thresholds you set and the trend statistics you collect are for the same server characteristics (CPU utilization, for example). The combination of threshold and trend statistics is a very useful troubleshooting tool.

To monitor trends as a troubleshooting tool, follow these steps:

Procedure 23

1. Set a threshold for the trend that you want to monitor.

After setting a threshold, you can let ManageWise monitor the trend until the trend passes the threshold value and sets off an alarm. Refer to "Setting Trends and Thresholds" on page 216.

2. When you receive an alarm, view the Alarm Report.

The Alarm Report lists when the alarm was received, the cause, and the severity of the alarm. If the alarm is due to a trend passing a threshold, continue to Step 3.

3. Correct the reason for the alarm.

The correction depends on the trend and threshold that caused the alarm. For example, you might monitor the amount of free Hot Fix Redirection Area available because that is an indicator of how well your server's hard disk is operating. If you receive an alarm telling you that the free Hot Fix Redirection Area available is below the threshold you set, you know that your hard disk is going bad.

The following sections describe how monitoring thresholds and trend statistics can help you when troubleshooting a problem:

◆ "Monitoring Free Hot Fix Redirection Area" on page 208

◆ "Monitoring Volume Usage" on page 208

◆ "Monitoring Number of Logged-in Users" on page 208

◆ "Monitoring CPU Utilization" on page 209

◆ "Monitoring Cache Buffers" on page 209Cache buffers

◆ "Monitoring Dirty Cache Buffers" on page 209

◆ "Monitoring File Cache Hits" on page 210

Monitoring Free Hot Fix Redirection Area

By monitoring the free Hot Fix Redirection Area, you can determine whether your server's hard disk is going bad. The free Hot Fix Redirection Area is a portion of disk space set aside for data blocks from faulty data blocks on the server's hard disk. The more free Hot Fix Redirection Area used, the more faulty data blocks on the server's hard disk and the lower the percentage of free redirection area.

The default threshold value is 50 percent. When this threshold is reached, the hard disk might start losing data.

Monitoring Volume Usage

In addition to monitoring free space on a volume as a planning tool (refer to "Monitoring Free Space on a Volume" on page 204), you can monitor free space as a troubleshooting tool. This is particularly useful if free space on a volume suddenly drops below a set threshold (for example, when a user backs up files to the monitored volume).

The default threshold value is 10 percent. When this threshold is reached, you should first determine whether the lack of free space is due to a user dumping data. If so, the data can probably be removed, increasing the free space. If the lack of free space was planned (by viewing long-term trends and estimating when the server would need more memory), increase the free space by adding a hard disk.

Monitoring Number of Logged-in Users

Setting a threshold, and monitoring the average number of logged-in users, can help you detect when you might have too many users for the server.

The default threshold value is 100 percent. When this threshold is reached, you should either obtain an additional license, increasing the number of users allowed on the server, or move some users to another server.

You can view long-term trends to plan your actions. To do this, follow the steps shown in "Monitoring the Number of Users on NetWare 3 Servers" on page 206.

Monitoring CPU Utilization

Setting a threshold, and monitoring the average CPU utilization percentage, can help you detect possible problems with the server. Usually, a server's CPU utilization stays between 10 percent and 50 percent. If a server's CPU utilization reaches 70 percent or higher, users start experiencing delays when accessing the server.

The default threshold value is 80 percent. When this threshold is reached, use the Server Monitor program (from either an RCONSOLE session or from the server's system console) to determine the NLM causing the high utilization. After you have identified this NLM, you can unload it or replace the CPU with a more capable one.

Monitoring Cache Buffers

Setting a threshold, and monitoring the percentage of free cache buffers available from the Cache Buffer pool, can help you determine when you should perform a memory upgrade to the server. When a NetWare server starts, memory is allocated to the Cache Buffer pool. As NLM files are loaded, this memory (called free cache buffers) decreases. The more NLM files loaded, the less free cache buffers available.

The default threshold value is 40 percent. When this threshold is reached, you should increase the amount of server RAM.

Monitoring Dirty Cache Buffers

Setting a threshold, and monitoring the average percentage of dirty cache buffers, can help you detect possible problems with the server. The average percentage of dirty cache buffers refers to the average percentage of file cache buffers that contain data, which must be written to the disk, from the previous sampling period. Usually, data from the file cache buffers is written to the disk almost immediately. If data accumulates in the file cache buffers, which causes the average percentage of dirty cache buffers to rise, the efficiency of disk accesses is questionable.

The default threshold value is 90 percent. When this threshold is reached, the problem could be with a disk I/O channel (the channel might not be fast enough to process the packets). View the File System Reads and File System Writes trends. If the values for these trends are at a maximum, replace the disk I/O board.

Monitoring File Cache Hits

Setting a threshold, and monitoring the average percentage of file system cache hits, can help you determine whether you should increase the server's RAM. A cache hit measures the number of times the server found requested data in RAM rather than having to go to the hard disk because the data was not in RAM. If the amount of RAM left after loading NLM files is small, the number of cache hits goes down.

The default threshold value is 50 percent. When this threshold is reached, you should increase the amount of RAM.

Troubleshooting Servers

Although the previous two sections list methods for planning and troubleshooting a server, they do not demonstrate how to troubleshoot a server with an unknown problem. You can use the following examples as guidelines for troubleshooting a server. Because problems you might encounter are defined in general terms (the server is slow, for example), you might check a number of server parameters to discover the specific problem.

Server Is Slow

A slow server can be caused by a number of different factors. If you get a number of complaints that a particular server is slow, follow these steps:

Procedure

1. **Open the slow server's Configuration window.**

   For information about opening a server's Configuration window, refer to "Viewing File Servers" on page 165.

2. **Check the number of users.**

   The more users accessing the server, the slower the server becomes. Check the number of users by either double-clicking the Users icon or viewing the Users trend (refer to "Viewing Trends" on page 212).

3. **Check the number of connections.**

   As with the number of users, the number of connections can affect the speed of the server. Check the number of connections by either double-clicking the Connections icon or viewing the Connections trend.

4. **Check the traffic coming in and going out of the server.**

The traffic can be affected by a number of factors.

◆ Cache Buffers not big enough—View the Cache Buffer trend from the Memory icon (refer to "Viewing Trends" on page 212). If the cache buffer is too small, you can allocate more memory using the NetWare SET command (refer to "SET Server Parameters" on page 220).

◆ Not enough RAM—View the File Cache Hits trend. If the number of cache hits is low, you do not have enough RAM.

◆ Bad disk I/O channel—View the Dirty Packets Received trend and the File Received and File Transmitted trends. You have a bad disk I/O channel if the server has a high percentage of dirty packets received and the server is receiving and transmitting at its maximum.

5. **Check the CPU utilization.**

View the CPU Utilization trend (refer to "Viewing Trends" on page 212). If the utilization is constantly high, you can redistribute processes to other servers to reduce the utilization or upgrade to a more powerful CPU.

Low Free Space on Volume Message Appears

This example assumes that you set a threshold to warn you that there is not much free space left on the volume (refer to "Setting Trends and Thresholds" on page 216 and "Monitoring Volume Usage" on page 208). If you receive a Low Free Space on Volume message, follow these steps:

Procedure
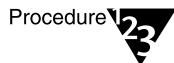
1. **Find the server on the internetwork map or segment map.**

The map shows a bell icon next to the server that caused the alarm.

2. **Double-click the server.**

The server's Configuration window is displayed.

3. **Double-click the Volumes icon.**

The Volumes detailed display window is displayed.

4. **Check the amount of free space on the volume.**

5. **If the amount of free space is minimal, add a hard disk to the server or move files to other servers to add free space to the volume.**

6. **If there is free space available, click the Trends action bar button.**

   If the Volumes table shows there is sufficient memory, someone dumped enough data to the volume to cause the alarm, and then removed it from the volume. You can confirm this by clicking the Trends action bar button to display the Free Space on Volume trend and finding where the free space dropped below the threshold.

Viewing Trends

Users can view trends from the View All File Servers window, Configuration window, or the component display of the Server detailed display window. You can view from one to four trends at one time. Trends can be displayed in a single graph or in multiple strip charts.

There are a number of features that are not apparent. These features follow:

◆ If you select more than one trend to view, the trend graph window that appears displays each trend as a stripchart with its own y-axis and title. Initial scaling of the trend graph is performed automatically from the trends data points. This is the default. To combine them into one graph, click the Multiple Line Graph button. This button, as well as the other graph control buttons, is described in the online help.

◆ You can click a point of the trend graph and see the value of the data at that point in the legend.

◆ Historical graphs have titles that show a date. This date corresponds to the beginning or left side of the graph.

◆ When you look at long-term trend graphs, you can click a point and increase the detail (zoom in) by decreasing the trend length. For example, if you see something interesting while viewing a weekly trend and you want to see a more detailed view, click the point of

interest and select the daily trend. The graph detail increases and the cursor remains on the point that you clicked.

Similarly, you can decrease the detail (zoom out) by increasing the trend length. For example, if you are viewing an hourly trend graph and you want to see what a trend did over the course of the week, you can select the weekly trend. The graph detail decreases to a view of the trend for the week.

When you zoom in or zoom out, the starting times and ending times of graphs are fixed. The starting times and ending times are as follows:

- **Zoom in from yearly historical graph to monthly historical graph**—Beginning the first of the month and ending 30 days after the first. For example, zooming in to May shows a trend from May 1 through May 30.

- **Zoom in from yearly or monthly historical graph to weekly historical graph**—Beginning Sunday of the week through the ending Sunday of the week.

- **Zoom in from yearly, monthly, or weekly historical graph to daily historical graph**—Beginning midnight of the selected day's morning through midnight of the selected day's evening.

- **Zoom in from yearly, monthly, weekly, or daily historical graph to hourly historical graph**—Start of the selected hour to the next hour.

◆ The first time you look at a long-term trend it might take a while for the trend to appear, especially if the trend contains many data points (a yearly trend, for example). When the trend appears, getting data is instantaneous because the data is cached. Therefore, if you find an interesting point on a yearly trend and you select the weekly trend to see more detail, the weekly trend graph appears with little or no delay.

Note   There is a delay if you go from a detailed trend graph (a weekly trend, for example) to a less detailed trend graph (a yearly trend, for example) because additional data must be accessed.

◆ You can use the scroll bar or scroll arrows at the bottom of the Trend Graph window to view trends that fall outside of the current time period of the graph. For example, while viewing a daily trend, you might want to see the trend for the day before. Using the scroll bar, you can move to the previous day's graph, four hours at a time.

Using a scroll arrow, you can move to the previous day's graph, a day at a time. This allows a continuous view of the server's performance. Table 8-19 shows the intervals moved when using the scroll arrows or the scroll bar.

Table 8-19
Scroll Intervals When Using the Scroll Arrows or Scroll Bar

Historical Trend	Scroll Arrow	Scroll Bar
Hourly	1 minute	1 hour
Daily	4 hours	1 day
Weekly	1 day	1 week
Monthly	1 day	30 days
Yearly	1 week	1 year

To view trend data, follow these steps:

Procedure
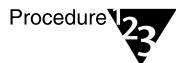
1. **Select a server to view.**

2. **Click the Trends button on the action bar or select *View > Trends*.**

   The Configure Trends dialog box, shown in Figure 8-19, is displayed. The dialog box displays a complete list of trends, as well as help for the Configure Trends dialog box.

Note

From the Configuration window, you can view trends specific to a portion of the server's configuration. For example, by clicking the Volumes icon and then clicking the Trends action bar button, you see only trends associated with volumes on the server.

From a detailed display window, you can achieve the most specific view of a trend. For example, to look at a specific volume, SYS:\ for example, click the SYS:\ volume in the Volume detailed display window, then click the Trends action bar button. Only the trend for the SYS:\ volume is displayed.

Figure 8-19
Configure Trends
Dialog Box
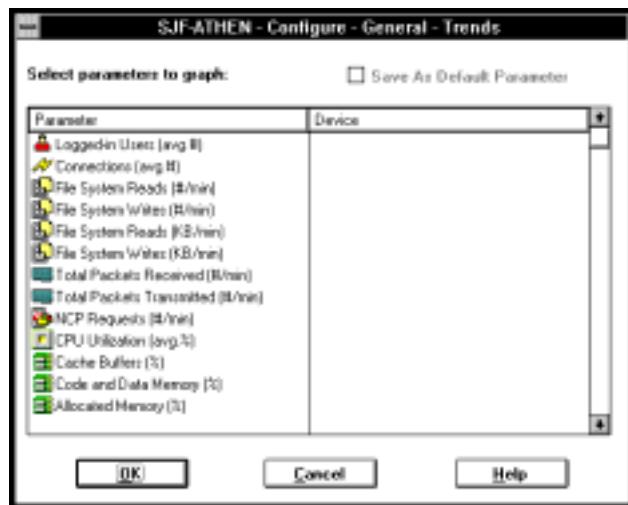
3. **Select one or more trends to display.**

   From the list of trends, you can select any combination of trend data to display in a graph. You can plot a maximum of four trends in a graph at one time.

4. **Click OK.**

   A trend graph, displaying your selected trends, appears on the screen. If you selected a number of trends, the screen displays each trend in a strip chart format.

Note ▼ You might see a discontinuity in the graph or graphs shown. Discontinuities indicate that either the server was down or samples taken to plot the graph were invalid. Large discontinuities in a graph are mostly due to the server being down. Small discontinuities, a missing point for example, are due to an invalid sample or set of invalid samples.

Changing Default Trend View Settings

Trends show a default graph when you click the Trends action bar button. For example, the default trend graph for Network Interfaces is Total Packets Received (#/min). You might want to change the default so you can view packets received for a single network interface.

To change a trend's default view, follow these steps:

1. **From the server's Configuration window, select an icon.**

2. **Click the Trends action bar button.**

   The default Trend graph is displayed.

3. **Click the Configure Active Window button.**

   The Configure Trends dialog box is displayed.

4. **Click the parameter you want as a new default.**

5. **Select Save As Default Parameter.**

6. **Click OK.**

Setting Trends and Thresholds

Trends and thresholds are very useful tools for planning and troubleshooting servers. Two sets of trend data are taken for every trend parameter. One set, sampled more often than the other set for a shorter duration, shows the current trend. The other set, sampled less often and for a longer duration, shows long-term trends (hourly, daily, weekly, monthly, and yearly).

Although all the trends are enabled, not all the thresholds are enabled. To see a complete list of trends and thresholds, and to determine whether a threshold is enabled, click the Threshold action bar button or select *Performance > NetWare Server Thresholds* from the View All Servers window.

You might want to enable currently disabled thresholds to warn you when these trends reach what you consider a critical point. For example, you might enable a threshold for the Ready Jobs in Queue (avg. #) trend because you know from experience that when the number of ready jobs in a queue reaches the threshold point, users begin to complain about a slow printer. You might also want to change a currently enabled threshold, or the sampling interval and trend length of a threshold, to more accurately reflect your server.

To enable a threshold, or to change the setting of a threshold or trend, follow these steps:

Procedure 22

1. **Select a file server.**

2. **Click the Trend and Threshold action bar button or select** *Performance > NetWare Server Thresholds*.

   The General Trends and Thresholds window, shown in Figure 8-20, is displayed. The window displays a complete list of thresholds.

Figure 8-20
General Trends and Thresholds Window

The number of trends and thresholds that you view from the General Trends and Thresholds window varies. When you view trends and thresholds from the View All File Servers window, every trend and threshold is shown for the selected server. When you view trends and thresholds from the Configuration window, trends and thresholds for the selected object group are shown (all volumes on a server, for example). When you view trends and thresholds from the server's detailed display window, only the object's trends and thresholds are shown (the volume SYS:\, for example).

If a threshold alarm is set, a red flag appears in the threshold column of the parameter that caused the alarm.

3. **Select a parameter, by clicking the Change Trend and Threshold Entry action bar button or double-clicking the parameter.**

   To set more than one parameter, hold down the Ctrl key while selecting the parameters, then click the Change Trend and Threshold Entry action bar button.

   The Trends and Thresholds Setup dialog box, shown in Figure 8-21, is displayed.

Figure 8-21
Trends and Thresholds Setup Dialog Box
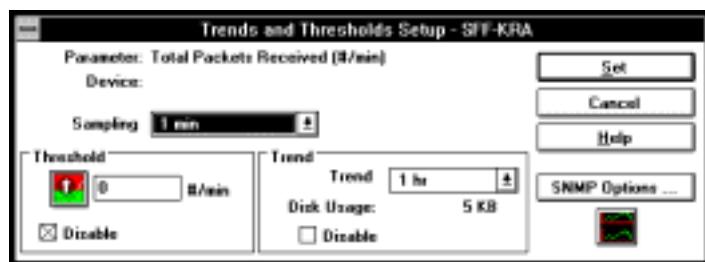
4. **Change the settings for the trend and threshold parameter.**

   You can change the following settings:

   ◆ **Sampling**—Interval over which data is averaged and stored. The number of times ManageWise samples a parameter is predetermined. Select one of the sampling intervals provided in the list box.

Suggestion   To increase the resolution for a current trend, change the sampling interval from 1 minute to 30 seconds or less.

Important   Keep the sample interval for current trends smaller than the sample interval for long-term trends. The default sample intervals are 1 minute and 15 minutes for most current trends and most long-term trends, respectively.

Note   Increasing the frequency of the sampling interval increases the amount of disk space required to store collected data.

   If you change the sampling interval, you lose trend data previously collected. If you want to save previously collected trend data, export the

data to a file. For information about exporting files, refer to *ManageWise 2.6 Setup Guide*.

◆ **Threshold**—Value that, when surpassed, triggers an alarm. Whether a parameter's value must rise or fall to trigger an alarm is predetermined and cannot be changed. ManageWise indicates a rising or falling threshold with an up or down arrow.

You can enable or disable a threshold using the Disable option.

◆ **Trend Length**—How much data is stored. The longer the trend length is, the more data is stored on the disk. The amount of disk space used to store the trend data is shown next to the Disk Usage heading. Select one of the trend lengths provided in the list box.

ManageWise writes newly gathered data over the oldest stored data, after the trend length is exceeded. For example, if you set a trend length of 3 months, 3 months ago, ManageWise begins overwriting the oldest data in the trend's database.

You can enable or disable a trend using the Disable option.

Note ◆ Disabling a trend does not disable an enabled threshold. A disabled trend passing the enabled threshold still triggers an alarm.

Changing the trend length has no effect on previously gathered data.

5. Click OK.

Note ◆ There is an inconsistency between threshold values you set below 1 minute and the value shown in the Trends and Thresholds Setup dialog box for thresholds whose statistics are measured by the minute (File System Reads, File System Writes, File System Reads (KB), File System Writes (KB), Packets Received, Packets Transmitted, Packets Received (KB), Packets Transmitted (KB), Total Packets Received, Total Packets Transmitted, and NCP Requests).

For example, if you sample File System Reads at 5-second intervals and set a threshold of 50, the threshold value shown in the Trends and Thresholds Setup dialog box is 48.

From the Trends and Thresholds Setup dialog box, you can also change the server's SNMP community string. The SNMP community string is a security precaution that prevents an unauthorized user from either receiving parameter data from the server or changing server parameter values. Refer to "Setting the Community Strings" on page 329 for more information regarding SNMP security.

Note ▼ Click the Graph icon to view the current trend graph for the selected trend and threshold parameter. You can use the graph as a visual aid when you set a threshold value.

Retrieving Trend Data

You can retrieve trend data manually or automatically from one or more manageable NetWare servers. Manual mode of retrieving trend data is performed when the Retrieve! button is clicked. Then, the trend data is retrieved immediately for the specified profile. In the scheduled mode of retrieving data, a schedule for the retrieval process is created and saved.

To start the Trend data retrieval process, select NetWare Server Trends from the Tools Menu in the ManageWise Console.

You must create Trend profiles to be able to retrieve data. The trend profiles contain information on

◆ scheduling the trend retrieval process

◆ selecting trend objects

◆ selecting NetWare servers to retrieve trend data

For more information on creating trend profiles, retrieving data, and intrepreting the output files, refer to the Help menu and field descriptions.

SET Server Parameters

NetWare server parameters control the memory allocations of the server, monitor the server's performance, and control workstations' use of the server's resources. With ManageWise, you can set parameters directly from the user interface.

For detailed server parameter information, refer to the SET command discussion in *Utilities Reference* in your NetWare server documentation.

To set server parameters, follow these steps:

Procedure 23

1. **Select a file server.**

   You can select the file server from the All NetWare File Servers window, from the file server's Configuration window, or from any map on which the file server appears.

2. **Click the SET Parameter action bar button or select** *Configure > NetWare File Server Parameters*.

   The Set Commands window, shown in Figure 8-22, is displayed. Server parameters are divided into groups. These groups are listed in a tree structure.

Figure 8-22
Set Commands
Window
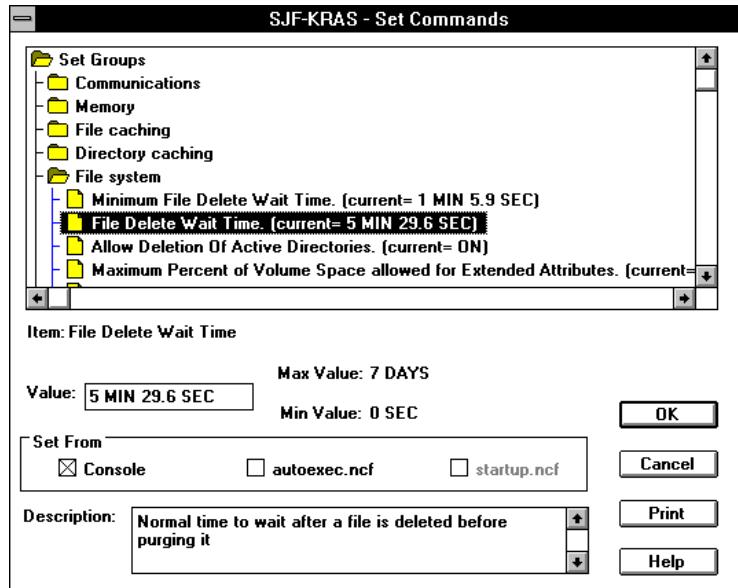
3. **Double-click a parameter group.**

   The selected parameter group expands, showing all the parameters that can be set, as well as the current value for each parameter.

4. **Click a parameter.**

The selected parameter is highlighted and listed in the Item field of the Set Parameters window. Values for a parameter are based on either a number (maximum packet receive buffers, for example), an amount of time (delay between watchdog packets, for example), or whether the parameter is on or off (console display watchdog logouts, for example). The description box lists a brief description of the parameter.

5. **Enter a new value in the Value field.**

6. **In the Set From box, select Console, AUTOEXEC.NCF, or STARTUP.NCF.**

   Depending on the parameter you select, either the Console and AUTOEXEC.NCF options are available or the STARTUP.NCF option is available.

   Selecting Console immediately configures the operating system to the new setting. The new setting is not permanent and is reset to its previous value when you restart the system.

   Selecting AUTOEXEC.NCF makes the change permanent by saving the new value in the AUTOEXEC.NCF file.

Note ▼ You can make the change immediate and permanent by selecting both the Console and AUTOEXEC.NCF options.

   Selecting STARTUP.NCF makes the change permanent by saving the new value in the STARTUP.NCF file. The new setting is not implemented until you restart the system.

7. **Repeat Step 3 through Step 6 for every parameter you want to change.**

8. **Click OK.**

   The Confirm Set Parameters dialog box is displayed. Listed in the dialog box are the parameters that you want to change, the new settings you selected, and the current parameter settings. Verify that all your parameter settings are correct.

9. **If you must modify the server's SNMP community string, select SNMP Options; otherwise, go to Step 10.**

   For information regarding SNMP community strings, refer to "Setting the Community Strings" on page 329.

10. Select Commit All.

This resets the server's parameters.

From the Set Commands window, you can print all the SET parameters or just the SET parameters in one of the groups. To print SET parameters, follow these steps:

Procedure

1. Click the Print button.

The Print dialog box is displayed. If you selected a group before clicking the Print button, that group is highlighted in the Print dialog box.

2. Select the groups you want printed.

You can select additional groups by clicking the group names. If you selected a group and you do not want it selected, click the group name again. If you want to print all the groups, go to Step 3.

3. Click either the Print button or the Print All button.

Clicking the Print button prints the SET parameters for the groups you selected. Clicking the Print All button prints all the SET parameters.

c h a p t e r

9 *Managing Workstations*

The ManageWise® Console enables you to manage remote workstations and view configuration information and statistics for workstations on network segments. In particular, you can

◆ Run programs on a remote workstation, transfer files between the ManageWise Console and a workstation, and restart a remote workstation. For information about these and other management tasks involving remote workstations, refer to *ManageWise 2.6 Desktop Management Guide.*

◆ Learn how a workstation is configured (its network and MAC addresses, mapped drives, and so on) and view a record of its incoming and outgoing packet traffic. To view this information, refer to "Monitoring Workstation Configuration" on this page.

◆ View packet and connection statistics for IPX™, SPX™, and a workstation's LAN driver. To view this information, refer to "Monitoring NetWare Client Statistics" on page 227. This section also helps you interpret these statistics for the purpose of troubleshooting workstations on your network.

This chapter also provides troubleshooting help for cases in which you are unable to access a particular workstation.

Monitoring Workstation Configuration

To monitor a workstation, you must have NetWare® Client™ 1.2 or later software installed on your ManageWise Console, specifically the Desktop SNMP services. To install the Desktop SNMP software, refer to *NetWare Client for DOS and MS Windows User Guide.*

To display configuration information about a NetWare workstation, follow these steps:

1. Select a workstation from a map.

2. Select *File > Open > NetWare Client*.

The NetWare Client window, Figure 9-1, is displayed.

Figure 9-1
NetWare Client
Window
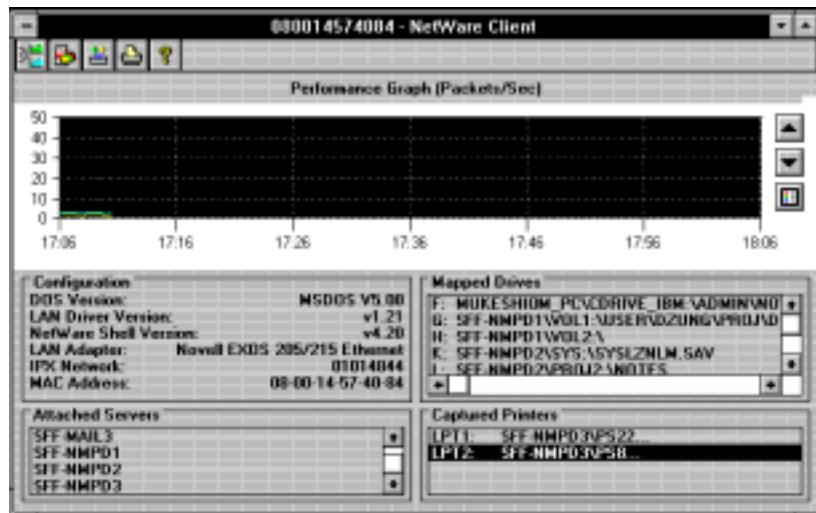
Note   You can open NetWare Client windows for as many workstations as you want, but only one NetWare Client window can be open for any given IPX address.

Below the action bar is the desktop graph. This displays a count of both good and bad packet traffic into and out of the workstation over the past hour.

The bottom half of the NetWare Client window shows four boxes, each of which has detailed information about how the workstation is set up:

◆ **Configuration box**—Displays the operating system (OS version) and network configuration information such as LAN driver version, NetWare Shell version, LAN adapter, IPX network, and MAC address.

◆ **Mapped Drives box**—Lists all the mapped network drives. The information is updated continually. Double-click the servers to open the Configuration window for servers.

Note ▼ All workstation VLM™ (Virtual Loadable Module™) files must be loaded for this information to be displayed.

WSDRVPRN.VLM provides mapped network drives and printers information. This VLM file is not shipped with NetWare Client 1.1; therefore, update to NetWare Client 1.2 or later if you want to see this information.

◆ **Attached Servers box**—Displays the names of the servers to which the client is attached.

◆ **Captured Printers box**—Lists all the printers to which the workstation is attached. The information here is updated continually.

Monitoring NetWare Client Statistics

ManageWise enables you to view the IPX statistics, SPX statistics, and LAN driver statistics. These statistics give you very detailed information about traffic into and out of NetWare clients. The following section presents guidelines that can help you make the best use of the client statistics to troubleshoot workstations.

Troubleshooting with Client Statistics

In general, when data is transmitted on the network, an acknowledgment is usually received. Therefore, when you are active at your workstation, you should see both the send and receive counts incrementing. The following diagram, in a simplified way, illustrates what the counters do:
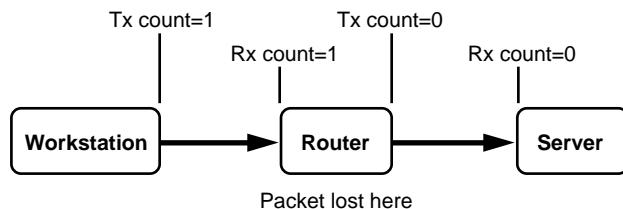
Under typical circumstances, Workstation A transmits to Server B, which acknowledges by sending a packet back to Workstation A. The operation increments Transmit A and Receive A. Thus, when there is a problem, you can use ManageWise to locate it. First, you can see

whether Workstation A is sending packets and getting a response. If Transmit A is counting but Receive B is not, the break is probably at Receive B or in the path between Transmit A and Receive B. If Transmit A is working but Receive A is not, the problem is likely to be Server B.

◆ A high count for any *send error* counter (such as the SPX Bad Send Packet Count) suggests a local problem, such as a board, driver, or application that might be sending bad packets. You can try swapping hardware or updating drivers, many of which are available on the NetWire® bulletin board.

◆ A high count for any *receive error* counter suggests a remote cause: a faulty application elsewhere on the network; faulty hardware or a bad intermediate machine; or, it could be a normal artifact of a protocol.

◆ A high retry count or lots of duplicate packets suggest several possibilities: a timeout length might be too short, there might be too much traffic on the segment, or a node might be jabbering.

◆ If a counter reaches a limit or any resources get exhausted, it could suggest that a node is jabbering. Use a network analysis device to check the network. Refer to Chapter 13, "Analyzing Your Network," for information about the ManageWise network analysis capabilities.

◆ If your retry rate is equal to your send rate, no packets are getting through successfully. The cause is likely to be a bad component on the wire. Check that the wiring is intact.

◆ A high error rate for the LAN driver counters suggests a problem with the network board. Try a different board to see whether the error rate decreases. If all the devices connected to a hub are experiencing the same problem, the hub or its cables might also be at fault.

In many cases, these statistics track parameters that are affected by settings in your NET.CFG file. For more information about the NET.CFG file, refer to *NetWare Workstation for DOS and Windows.*

To view the NetWare Client Statistics window, click the Statistics Window button in the NetWare Client window.

Figure 9-2
NetWare Client
Statistics Window

Type	Counter	Total	Rate
	00001B1E6C38 - NetWare Client Statistics		
IPX	Send Packet Count	7431	0
IPX	Malformed Packet Count	0	0
IPX	Get ECB Request Count	194196	0
IPX	Get ECB Failure Count	172797	0
IPX	AES Event Count	140276	0
IPX	Postponed AES Event Count	0	0
IPX	Max Configured Sockets Count	20	0
IPX	Max Open Sockets Count	10	0
IPX	Open Socket Failure Count	0	0
IPX	Listen ECB Count	20574	0
IPX	ECB Cancel Failure Count	0	0
IPX	Find Route Failure Count	0	0
SPX	Max Connections Count	15	0
SPX	Max Used Connections Count	1	0
SPX	Establish Connection Requests	0	0
SPX	Establish Connection Failures	0	0
SPX	Listen For Connection Requests	8	0
SPX	Listen For Connection Failures	0	0
SPX	Send Packet Count	17	0
SPX	Window Choke Count	0	0
SPX	Bad Send Packet Count	0	0
SPX	Send Failure Count	0	0
SPX	Abort Connection Count	0	0
SPX	Listen Packet Count	25	0
SPX	Bad Listen Packet Count	0	0

The counters start when you open the NetWare Client Statistics window.

The following sections list the IPX, SPX, and LAN Driver counters and explain each one.

Interpreting IPX Counters

IPX addresses and routes outgoing data packets across a network and incoming data packets to the proper area within a node's operating system. IPX counters, therefore, track node and network activity related to successful packet addressing. Table 9-1 lists IPX counters.

Table 9-1
IPX Counters

Counter Type	Explanation
Send Packet Count	Number of times IPX was called to send a packet.
Malformed Packet Count	Number of Send Event Control Blocks (ECBs) given to IPX with a fragment count of 0 or a first fragment size of less than 30 bytes.
Get ECB Request Count	Number of times IPX was asked for a receive ECB. This is the number of inbound packets given to IPX by the driver.

Table 9-1 *continued*
IPX Counters

Counter Type	Explanation
Get ECB Failure Count	Number of times IPX was unable to supply a receive buffer when asked to do so. The incoming packet was lost.
AES Event Count	Number of times IPX was asked to keep the AES (timer) ECB.
Postponed AES Event Count	Number of times IPX delayed servicing an event because at the time it wanted to service the event, IPX was in a critical section.
Max Configured Sockets Count	Maximum number of sockets IPX was configured to allow open simultaneously.
Max Open Sockets Count	Maximum number of sockets that have been opened simultaneously. If this counter is often close to the value of the Max Configured Sockets Count, increase the IPX SOCKETS value in your NET.CFG file.
Open Socket Failure Count	Number of times an IPX open socket request failed. An open socket request fails if the socket table is full or if the requested socket is already open.
Listen ECB Count	Number of times IPX was called with a listen ECB.
ECB Cancel Failure Count	Number of times IPX was unable to cancel an ECB because the target ECB was in use by a critical section.
Find Route Failure Count	Number of times IPX was unable to find a route to a requested network.

Interpreting SPX Counters

SPX verifies that the link between nodes is functioning and that packets are delivered by requesting verification from the destination that the packet was received. SPX counters, therefore, track network activity related to a healthy network link and successful packet delivery. Table 9-2 lists SPX counters.

Table 9-2
SPX Counters

Counter Type	Explanation
Max Connections Count	Maximum number of SPX connections that SPX is configured to support simultaneously. You can modify this value using the SPX CONNECTIONS parameter in the NET.CFG file.
Max Used Connections Count	Maximum number of connections that have been opened simultaneously.
Establish Connection Requests	Number of times SPX was called to establish a connection with a remote partner.
Establish Connection Failures	Number of times an SPX Establish Connection Request failed because the SPX packet header was too small, the SPX session table was full, or no router could be found to the target network.
Listen for Connection Requests	Number of times SPX was called to listen for a connection startup call from a remote partner.
Listen for Connection Failures	Number of times an SPX Listen for Connection Request failed because the SPX session table was full.
Send Packet Count	Number of packets SPX sent across an SPX session.
Window Choke Count	Number of times an SPX packet could not be sent across a connection because the SPX partner on the remote station had not yet allocated a receive buffer to accept the packet.
Bad Send Packet Count	Number of times SPX was asked to send a packet on a session that did not exist or was asked to send a packet with a first fragment size less than 42 bytes.
Send Failure Count	Number of times SPX was unable to successfully deliver and receive acknowledgment of a packet across an SPX connection. In this case, the SPX connection is aborted and the failure is reported to the sender.

Table 9-2 *continued*
SPX Counters

Counter Type	Explanation
Abort Connection Count	Number of times SPX was instructed to abort a connection without notifying the connection partner.
Window Choke Count	Number of times an SPX packet could not be sent across a connection because the SPX partner on the remote station had not yet allocated a receive buffer to accept the packet.
Listen Packet Count	Number of listen ECBs given to SPX.
Bad Listen Packet Count	Number of listen ECBs given to SPX that were rejected because they had no fragments, the first fragment was less than 42 bytes, or the socket they were to listen on was not open.
Incoming Packet Count	Number of arriving SPX packets.
Bad Incoming Packet Count	Number of arriving SPX packets that were discarded because of session failure. (There was no such active session or the packet was not from the session partner.)
Suppressed Packet Count	Number of arriving SPX packets that were discarded because they were duplicates of previously delivered packets.
No Session Listen ECB Count	Number of arriving SPX Establish Connection Requests that were unfilled because no matching SPX Listen for Connection Request was available.
Watchdog Destroy Session Count	Number of sessions destroyed by the watchdog because it could no longer communicate with the connection partner. (A watchdog ensures that resources are not consumed unnecessarily, as when the sender tries to send even though the destination is down.)

Interpreting LAN Driver Counters

A LAN driver is a file that understands and controls the physical structure of a network board. LAN drivers serve as a link between a station's operating system and the physical network parts. LAN driver counters, therefore, track network activity related to the successful delivery of packets between the operating system and the physical network. Table 9-3 lists LAN driver counters.

Table 9-3
LAN Driver Counters

Counter Type	Explanation
Total Tx Packet Count	Number of packets that have been transmitted successfully by the driver since the last reset or initialization. This count does not include transmissions that were terminated by an error.
Total Rx Packet Count	Number of packets successfully received by the driver since the last reset or initialization. This count does not include packets that were received but did not continue into the system due to an error.
No ECB Available Count	Number of packets received for which there was no listening ECB.
Packet Tx Too Big Count	Number of times the driver was requested to transmit a packet that was larger than the largest size packet that can be transmitted.
Packet Tx Too Small Count	Number of times the driver was requested to transmit a packet that was smaller than the smallest size packet that can be transmitted.
Packet Rx Overflow Count	Number of times the packet received from the network was larger than the size of the buffer allocated to receive it.
Packet Rx Too Big Count	Number of times the packet received from the network was larger than the largest size packet that can be transmitted on the system. Collisions occasionally create these, as can servers that are testing the intermediate links.
Packet Rx Too Small Count	Number of times the packet received from the network was smaller than the smallest size packet that can be transmitted on the system.
Packet Tx Misc Error Count	Number of miscellaneous errors that prevented a packet from being transmitted.
Packet Rx Misc Error Count	Number of miscellaneous errors that prevented a packet from being received.
Retry Tx Count	Number of times the system retried a packet transmission. For example, on a transmission collision, the driver tries again to transmit the packet.
Checksum Error Count	Number of checksum errors that occurred while receiving packets.
Hardware Received Mismatch Count	Number of times the hardware received more bytes or fewer bytes than expected.

Troubleshooting NetWare Client

If you cannot monitor workstations, ensure that NetWare Client software is installed on your ManageWise Console and that the following statements are included in your NET.CFG and STARTNET.BAT files.

In the DOS REQUESTER section of the NET.CFG file, ensure that the following statements are included:

```
VLM = WSSNMP.VLM
VLM = WSREG.VLM
VLM = WSTRAP.VLM
VLM = WSASN1.VLM
VLM = WSDRVPRN.VLM
```

In the Transport Provider IPX section of the NET.CFG file, ensure that the following statement is included:

```
TRAP TARGET = IPX address:Node address
```

The trap target address is the address of the ManageWise Console.

In the STARTNET.BAT file, ensure that the following is included after the VLM.EXE line:

```
STPIPX.COM
```

If you have a Novell® TCP/IP network, or if you want to send traps to a UNIX management console, you can use User Datagram Protocol (UDP) as the transport provider. In this case, you add the following statements to the NET.CFG file:

```
TRANSPORT PROVIDER UDP
TRAP TARGET = x.y.z.w
```

The trap target address is the IP address of the ManageWise Console or UNIX management console.

To run the SNMP-UDP transport interface at startup, add the following statement after the VLM.EXE line in the STARTNET.BAT file:

```
STPUDP.COM
```

chapter **10** *Managing Routers*

Routers are indispensable in building your internetwork. They attach to network segments and forward traffic, as needed, from one segment to another. To manage your network effectively, you need to know what routers exist in your internetwork and their operating status.

ManageWise® software provides the internetwork map described in Chapter 2, "Using Maps," which gives a graphical view of where network segments are connected through routers. This chapter describes a facility that lists those routers in a summary format. At a glance, this summary displays an inventory of the routers and the number of segments each router is connected to. On demand, ManageWise gives a software description of the router and its operating status. Starting with the summary, ManageWise then gives you access to the following detailed information:

◆ **Traffic statistics**—You can monitor the statistics about traffic that routers exchange with each attached segment. The statistics collected enable you to characterize the use of network adapter cards in forwarding traffic.

◆ **IPX™ routers**—You can monitor the status of IPX routers. You can view information about how each IPX router is configured, what circuits are attached, and how much traffic each router is receiving and sending. This information is useful for troubleshooting and load balancing. You can also use this information if you want to reconfigure your routers using RCONSOLE (refer to Appendix A, "Using Remote Console," for more information).

◆ **Pathways**—You can view the path between two routers. ManageWise displays the path in both directions. Although the two paths are usually identical, they can differ on complicated networks or when an intermediate link is malfunctioning. By asking ManageWise for path information, you can identify the malfunctioning router or segment.

◆ **NLSP™ information**—You can access the IPX routers that are running NLSP. You can view information about IPX routers and networks in an NLSP area and view the shortest path between any two.

These statistics help to identify busy segments and serial links in your internetwork and to find problems and the segments on which they are generated. You can use ManageWise facilities to document your network, which will help you track growth and plan for future expansion.

Displaying Global Routers Summary

After you start ManageWise, you can use the menus and commands in the ManageWise main window to display information about all the routers in your network.

To display a global summary of routers in the ManageWise database, select *View > All > Routers* from the main menu bar. The Routers summary table, Figure 10-1, is displayed. When the table first appears, only the Router Name and Routed Protocols columns have data. Select one or more routers, and then click the Query action bar button to obtain data for the other columns.

Figure 10-1
Routers Summary Table

The Routers summary table complements the ManageWise internetwork map by providing a list of all routers that connect your internetwork. Static configuration information, such as the router names and number of known interfaces, is retrieved from the ManageWise database. Dynamic information, such as the time since the router was brought up, is retrieved from the routers using SNMP.

Note ▼ The Routers summary table might not display information about a router that is currently running but was not up when the NetExplorer™ software was discovering the network.

Table 10-1 explains the fields in the Routers summary table.

Table 10-1
Routers Summary Table Fields

Field	Explanation
Router Name	Name of the router.
Routed Protocols	Protocols the router uses to communicate with other routers. This information is obtained from the ManageWise database.
Last Query Time	Last time the router was polled.
Supported MIBs	Information about whether the router supports SNMP MIB-I, MIB-II, IPX, AppleTalk*, or Bridge MIB. If the router does not support these MIBs, or is not operational at the time, this field is blank.
Description	Description of the router, as supplied by the manufacturer.
Up Since	Date and time the router was most recently started. The date and time are relative to the ManageWise workstation. If a router is not operational or is not SNMP-compatible, this field displays the value No SNMP Support.
# Segments	Number of segments the router was connected to when the network topology was discovered. This information is obtained from the ManageWise database.
Vendor	Name of the vendor. This information is obtained dynamically through the query, not from the ManageWise database. If you want the ManageWise database to contain this information, you must add it manually using the Database Object Editor. If this data cannot be obtained through the query, this field is blank.

Table 10-1 *continued*
Routers Summary Table Fields

Field	Explanation
Location	Physical location of the router. This information is obtained dynamically through the query, not from the ManageWise database. If you want the ManageWise database to contain this information, you must add it manually using the Database Object Editor. If this data cannot be obtained through the query, this field is blank.
Contact	Contact for the router. This information is obtained dynamically through the query, not from the ManageWise database. If you want the ManageWise database to contain this information, you must add it manually using the Database Object Editor. If this data cannot be obtained through the query, this field is blank.

Monitoring Statistics for Node Interfaces

Using ManageWise, you can monitor node interface statistics for one or more nodes in the ManageWise database. An *interface* is an attachment, through a network adapter board, to a network segment. A router typically has multiple network attachments to route traffic in the internetwork.

Monitoring the interface statistics of a router enables you to know how the interfaces are used by the selected routers. You can also understand the traffic across a router and thereby identify busy segments in the network.

Interfaces Table

The Interfaces table displays active data. The active data is constantly refreshed, presenting real-time statistics.

Note ManageWise does not store the interface statistics. If you want to save the statistics for later review or comparison, use the Print or Export command, described in *ManageWise 2.6 Setup Guide*.

When you select a single router, the Interfaces table looks like the one in Figure 10-2. This figure does not display all the fields in the table. To view all the fields in the table, use the scroll bars and adjust the column widths as described in *ManageWise 2.6 Setup Guide*.

Figure 10-2
Node Interfaces Table

Interface	Type	Physical Address	Status	Pkts In/s	Pkts Out/s	Errors In Total	Errors Out Total	Discards In Total	Discards Out Total	Pk
1	Ethernet_II	00-00-1b-15-ea-ec	Up	195	204	20	0	0	0	
2	Ethernet_802.3	00-00-1b-15-ea-ec	Up	196	205	20	0	0	0	
3	Ethernet_II	00-00-1b-15-51-c5	Up	132	124	0	0	0	0	
4	Ethernet_802.3	00-00-1b-15-51-c5	Up	134	126	0	0	0	0	
5	Ethernet_II	00-00-1b-15-4a-07	Up	113	99	14	0	0	0	
6	Ethernet_802.3	00-00-1b-15-4a-07	Up	114	100	14	0	0	0	
7	Ethernet_802.3	00-00-1b-15-4a-07	Up	113	99	14	0	0	0	
8	FDDI	00-80-d8-20-52-ab	Up	349	346	0	0	0	0	
9	Ethernet_802.3	00-00-1b-3f-fb-c6	Up	3	7	0	0	0	0	
10	Ethernet_802.3	00-00-1b-3f-fb-c6	Up	3	7	0	0	0	0	
11	Ethernet_II	00-00-1b-3f-fb-c6	Up	3	6	0	0	0	0	

Window title: Active - SJF-DEV-MPR - Interfaces

When you select multiple routers, the Interfaces table displays the interface index together with the router name in the first column of each entry. The interface index is simply a way to identify an interface.

Note ▼ Some columns in the Interfaces table might display a value of zero. In some cases, a value of zero might mean that the data is not applicable. This is a limitation of your network adapter board or driver.

Chapter 10: Managing Routers   **241**

Table 10-2 explains the fields in the Interfaces table.

Table 10-2
Interfaces Table Fields

Field	Explanation
Interface	Interface index. If you select a single router, the table displays only the interface index. Most router vendors instrument each network interface adapter to be one interface, as shown in Figure 10-2. The Novell® NetWare® MultiProtocol Router™ product, however, supports the concept of logical interfaces. Each logical interface represents a networking protocol instance using a physical adapter, as shown in Figure 10-2. All logical interfaces describing a physical interface might display similar values. Some interface entries have physical address information, and you can use the values to identify the shared physical adapters.
Type	Media type of the interface, such as Ethernet.
Physical Address	Physical address of the interface. If an interface does not have a physical address, such as a serial line, this field is blank.
Status	Current operational state of the interface.
Pkts In/s	Number of packets received, per second, by the interface.
Pkts Out/s	Number of packets sent, per second, by the interface.
Errors In Total	Number of packets that could not be received because of errors. This number is accumulated since monitoring most recently started.
Errors Out Total	Number of packets that could not be transmitted because of errors. This number is accumulated since monitoring most recently started.
Discards In Total	Number of inbound packets discarded even though no errors were detected to prevent them from being received. This number is accumulated since monitoring most recently started. One reason for discarding such a packet could be a lack of receive buffer space.
Discards Out Total	Number of outbound packets discarded even though no errors were detected to prevent them from being transmitted. This number is accumulated since monitoring most recently started. One reason for discarding such a packet could be its exceeding the maximum packet limit of the transmit queue.
Pkts In Total	Number of packets received by the interface since monitoring most recently started.
Pkts Out Total	Number of packets transmitted out of the interface since monitoring most recently started.

Table 10-2 *continued*
Interfaces Table FIelds

Field	Explanation
Bytes In Total	Number of bytes received by the interface since monitoring most recently started.
Bytes Out Total	Number of bytes transmitted by the interface since monitoring most recently started.
Bytes In/s	Number of bytes received, per second, by the interface during the current monitoring period.
Bytes Out/s	Number of bytes transmitted, per second, by the interface during the current monitoring period.
Speed (Kbits)	Current bandwidth of the interface in kilobits per second (Kbps). If an interface varies in bandwidth, or if an accurate estimate of the bandwidth cannot be made, this field contains the nominal bandwidth.
Description	Description of the interface. This might include the name of the manufacturer, the product name, and the version of the hardware interface.

Router Interface Statistics Graph

Using ManageWise, you can plot router interface statistics. The router Interface Statistics graph displays activity on a per-interface basis. Each field in the Interfaces statistics table is identified on the graph with a different colored line.

To start the graph, follow these steps:

Procedure
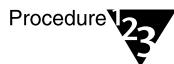
1. **Select an interface by clicking a row in the Interfaces statistics table.**

   The selected row is highlighted and the Graph action bar button is enabled.

2. **Click the Graph action bar button in the Interfaces statistics table.**

The Interface Graph Settings dialog box is displayed.

Interface Graph Settings

Interval: Samples to plot:

5 Sec   60

☐ Save settings

OK   Cancel   Help
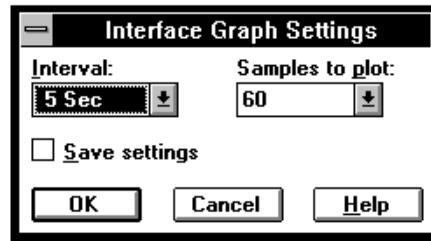
3. In the Interval field, specify how often to plot the data.

The interval you select is the time difference between two adjacent time marks.

4. In the Samples to plot field, specify the number of data samples to display in the window.

If the graph contains more data samples than ManageWise can plot in the horizontal axis, a scroll bar appears at the bottom.

5. Select the Save settings check box if you want to save the values you set in the dialog box so that all subsequent graphs use them.

6. Click OK.

ManageWise displays a graph of real-time statistics, as it is received, for the selected interface (refer to Figure 10-3). You can open additional graphs to depict traffic on different network segments.

Note   These statistics are not stored in the database. They are retained only while the graph is displayed. If you want to store the data for later review or comparison, use the Print or Export command, described in *ManageWise 2.6 Setup Guide*.

Figure 10-3
Router Interface
Statistics Graph
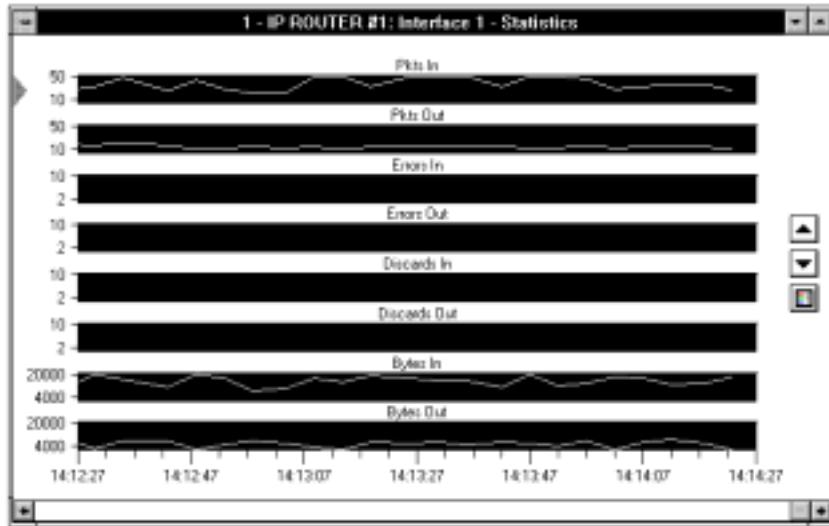
The following statistics are displayed:

◆ **Pkts In**—Rate, in packets per second, of packets received by the interface since monitoring most recently started.

◆ **Pkts Out**—Rate, in packets per second, of packets transmitted by the interface since monitoring most recently started.

◆ **Errors In**—Rate, in packets per second, of packets that could not be received because of errors.

◆ **Errors Out**—Rate, in packets per second, of packets that could not be transmitted because of errors.

◆ **Discards In**—Rate, in packets per second, of inbound packets discarded even though no errors were detected to prevent them from being received. A reason for discarding such a packet could be to free buffer space.

◆ **Discards Out**—Rate, in packets per second, of outbound packets discarded even though no errors were detected to prevent them from being transmitted. A reason for discarding such a packet could be to free buffer space.

◆ **Bytes In**—Rate, in packets per second, of data received by the interface since monitoring most recently started.

◆ **Bytes Out**—Rate, in packets per second, of data transmitted by the interface since monitoring most recently started.

You can optimize the display of incoming data using the buttons on the right side of the graph:

Vertical Axis Scale—Controls the scale of the selected graph. The scale values appear on the left edge of the graph.

Legend—Displays an explanation of the colors on the graph. You can toggle this button to display or remove the legend on the graph. You can obtain the statistical values of a particular sample by clicking the corresponding point on the time scale and then clicking the Legend button.

You can zoom in to any statistic by double-clicking it. The graph area of that statistic then expands to fill the window. To return to the original graph, double-click the window again.

Monitoring All IPX Routers

ManageWise provides the IPX Routers table, which you can use to monitor all IPX routers in your database and to get further management information on demand. The IPX Routers table lets you know what manageable IPX routers are in your network and also gives you information about them, such as their network addresses and routing protocols. An IPX router is manageable when it has IPX information instrumented to SNMP.

To display the IPX Routers table, follow these steps:

Procedure

1. **Display the global router summary by selecting** *View > All > Routers***.**

   The Routers summary table, Figure 10-1 on page 238, is displayed.

2. **Click the IPX Routers button in the action bar.**

   ManageWise collects the router data and displays the status in the window title as it does so. The IPX Routers table, Figure 10-4, is displayed. When the table first appears, only the Name and

Network Address columns have data. Select one or more routers, and then click the Query action bar button to obtain data for the other columns.

Note ▼ If your network includes dial-up lines, consider the cost of SNMP requests when determining how often to query routers reached over dial-up lines.

Figure 10-4
IPX Routers Table
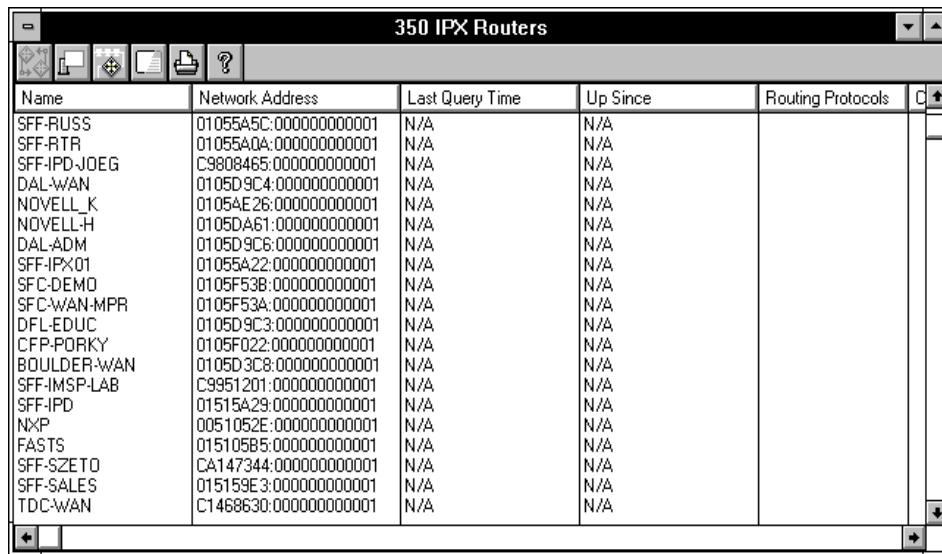
Name	Network Address	Last Query Time	Up Since	Routing Protocols	C
SFF-RUSS	01055A5C:000000000001	N/A	N/A		
SFF-RTR	01055A0A:000000000001	N/A	N/A		
SFF-IPD-JOEG	C9808465:000000000001	N/A	N/A		
DAL-WAN	0105D9C4:000000000001	N/A	N/A		
NOVELL_K	0105AE26:000000000001	N/A	N/A		
NOVELL-H	0105DA61:000000000001	N/A	N/A		
DAL-ADM	0105D9C6:000000000001	N/A	N/A		
SFF-IPX01	01055A22:000000000001	N/A	N/A		
SFC-DEMO	0105F53B:000000000001	N/A	N/A		
SFC-WAN-MPR	0105F53A:000000000001	N/A	N/A		
DFL-EDUC	0105D9C3:000000000001	N/A	N/A		
CFP-PORKY	0105F022:000000000001	N/A	N/A		
BOULDER-WAN	0105D3C8:000000000001	N/A	N/A		
SFF-IMSP-LAB	C9951201:000000000001	N/A	N/A		
SFF-IPD	01515A29:000000000001	N/A	N/A		
NXP	0051052E:000000000001	N/A	N/A		
FASTS	015105B5:000000000001	N/A	N/A		
SFF-SZETO	CA147344:000000000001	N/A	N/A		
SFF-SALES	015159E3:000000000001	N/A	N/A		
TDC-WAN	C1468630:000000000001	N/A	N/A		

Table 10-3 explains the fields in the IPX Routers table.

Table 10-3
IPX Router Table FIelds

Field	Explanation
Name	Name of the router.
Network Address	Router network address.
Routing Protocols	Routing protocols enabled; these are used among routers to communicate with each other. Obtained dynamically by SNMP.
CIrcuits	Number of circuits on the router. Obtained dynamically by SNMP.
Networks	Number of networks the router can send data to. Obtained dynamically by SNMP.
Services	Number of services announced by servers and kept track of by the router so it can route service request packets to them. A service is a function provided on the network, such as print services or file services. Obtained dynamically by SNMP.
Up Since	Date and time the router was most recently started.

To view details about any router in the table, double-click it to show the IPX Router Details window, which is explained in the next section.

Figure 10-5
Path Trace Window


```
┌─────────────────────────────────────────────────────────────────────┐
│ ▢        TDC-WAN-MPF <-> SFF-RTR - IPX Path Trace              ▼ ▲ │
├─────────────────────────────────────────────────────────────────────┤
│               Path from TDC-WAN-MPF to SFF-RTR                        │
│                                                                       │
│          RIP                RIP            1 intermediate router      │
│                                                                       │
│    TDC-WAN-MPF     SJF-FR-INTL-MPF    0101 5F01:              SFF-RTR │
│                          30           C0000C01C801                    │
│                                                                       │
├─────────────────────────────────────────────────────────────────────┤
│               Path from SFF-RTR to TDC-WAN-MPF                        │
│                                                                       │
│          RIP                RIP            1 intermediate router      │
│                                                                       │
│      SFF-RTR       SJF-DEV-MPF        0101 4000:          TDC-WAN-MPF │
│                                       C0000C17F8D8                    │
└─────────────────────────────────────────────────────────────────────┘
```
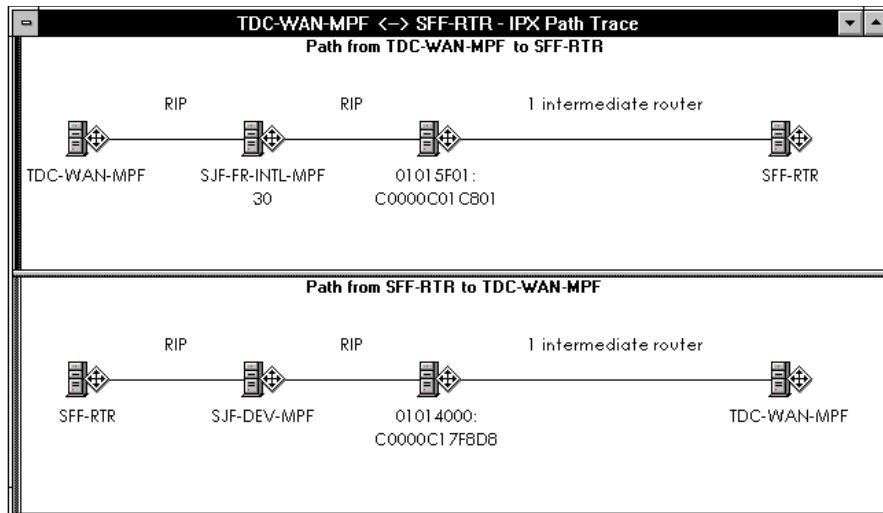
ManageWise queries the source router's forwarding table (through SNMP) for the next hop and repeats this process until it either reaches the destination or the next-hop router does not have the forwarding table instrumented under SNMP. ManageWise then displays a path for each direction; although the two paths are usually identical, they can differ on complicated networks or when an intermediate link is malfunctioning. By viewing path information, you might be able to identify the malfunctioning router or segment. However, differing paths do not necessarily indicate a problem.

If the path between the two routers includes a router that is not supplying the trace information this application queries, the path shown stops at that hop because ManageWise obtains trace path data dynamically through SNMP. However, by looking at the path tracings in both directions, you can usually determine the path.

Note   You can also select *Fault > Trace IPX Path* to invoke this function.

◆ **RCONSOLE**—Invokes RCONSOLE (refer to Appendix A, "Using Remote Console").

◆ **Go To**—Displays the ManageWise internetwork map (refer to "Internetwork Map Display Format" on page 31) and highlights the selected router.

◆ **Query**—Queries the router to obtain dynamic data, such as the date and time the router became operational and the networks to which the router can send data, routing protocols, circuits, and services.

◆ **Print**—Sends the IPX Router table to the printer.

◆ **Help**—Displays online help. This is equivalent to pressing the F1 key.

Viewing IPX Router Details

The IPX Router Details window gives you access to information about the configuration and statistics of manageable IPX routers.

Figure 10-6
IPX Router Details Window
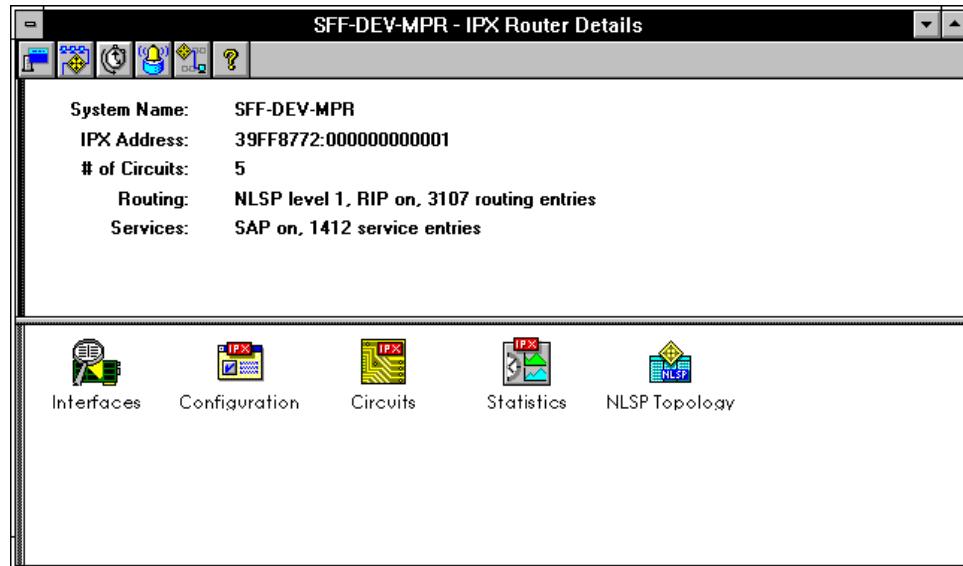
Below the action bar are the two panes of the IPX Router Details window. The top pane summarizes the router configuration:

◆ **System Name**—Name of the router.

◆ **IPX Address**—Network address.

◆ **# of Circuits**—Number of IPX circuits on the router.

◆ **Routing**—IPX routing protocols enabled on the router.

◆ **Services**—Number of services announced by servers and kept track of by the router so it can route service request packets to the servers.

If ManageWise cannot connect to the router, these dynamically obtained fields show the status *Unknown*.

The bottom window has the following icons:

◆ **Interfaces**—Displays a table listing and describing the router interfaces and giving real-time traffic information about each. This table is explained in "Router Interface Statistics Graph" on page 243.

◆ **Configuration**—Displays a dialog box with configuration information. This dialog box is explained in the following section.

◆ **Circuits**—Displays a table describing the IPX connections the router has. This table is described in "Viewing Router IPX Connections" on page 256.

◆ **Statistics**—Displays a graph showing real-time IPX statistics on incoming and outgoing packets. This graph is described in "Viewing IPX Statistics for a Router" on page 258.

◆ **NLSP Topology**—Displays a window showing information about the NSLP area immediate to the router. This window is explained in "Monitoring NLSP Routers" on page 260.

Viewing Configuration Data for an IPX Router

The IPX Router Configuration window gives you specific information about how the IPX protocol is configured on the router. To see the IPX Router Configuration window, double-click the Configuration icon in the IPX Router Details window (Figure 10-6 on page 250). The IPX Router Configuration window, Figure 10-7 on page 252, is displayed.

Figure 10-7
IPX Router Configuration Window
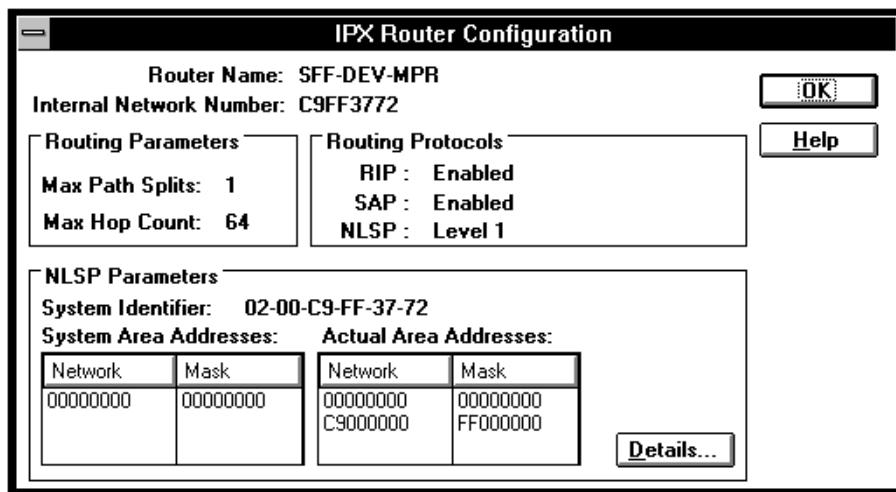
The window displays the following information:

◆ At the top are the router name and internal network number.

◆ The Routing Parameters box lists two parameters:

  ◆ **Max Path Splits**—Maximum number of paths a packet can take to reach the same destination.

  ◆ **Max Hop Count**—Maximum number of routers a packet can pass through before being discarded.

◆ The Routing Protocols box shows the status of the RIP, SAP, and NLSP protocols.

The bottom half of the window shows the NLSP Parameters (these are grayed out if the router is not running NLSP).

◆ **System Identifier**—Unique identifier for the router.

◆ **System Area Addresses**—Four-byte hexadecimal number that identifies the area addresses configured into the router.

◆ **Actual Area Addresses**—Four-byte hexadecimal number that identifies the addresses in the router's area.

Inside the NLSP Parameters box is the Details button, which you can click to display the Detailed NLSP Parameters window (Figure 10-8).

Figure 10-8
Detailed NLSP
Parameters Window
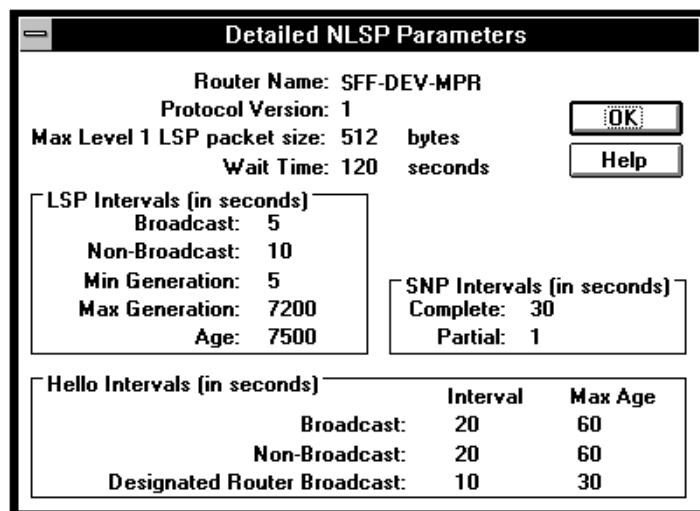
The following information is displayed in the window:

◆ **Router Name**—Router name.

◆ **Protocol Version**—Version of NLSP on the router.

◆ **Max Level 1 LSP packet size**—Maximum size, in bytes, of the link state packet.

◆ **Wait Time**—When a router's link state database becomes overloaded, the router informs other routers about its condition and enters a *wait state*. While in this state, the router does not route, which frees its resources. When the wait time has elapsed, the router returns to its normal state and informs other routers that it can route again.

◆ **LSP Intervals**—Five intervals are listed, all measured in seconds:

 ◆ **Broadcast**—Minimum time interval at which the router broadcasts a link state packet over a broadcast circuit, which is a LAN such as Ethernet, token ring, or FDDI.

 ◆ **Non-Broadcast**—Minimum time interval at which the router broadcasts a link state packet over a non-broadcast circuit, such as a WAN link.

 ◆ **Min Generation**—Minimum interval at which the router generates a local link state packet because of network changes or problems, such as bouncing links, changing cost of a route, and neighbor state changes.

 ◆ **Max Generation**—Maximum interval at which the router generates a local link state packet. This is the frequency with which LSPs are generated when there are no changes in the LSP. This value should be at least 300 seconds less than the aging interval.

 ◆ **Age**—Maximum number of seconds the router keeps a link state packet it has received from another router. If a new LSP is not received before this time expires, the LSP is removed from the router's database. This allows permanently disabled routers or networks to be removed from the database.

◆ **SNP Intervals**—Two intervals are listed, both in seconds:

 ◆ **Complete**—Time interval at which the router sends Complete Sequence Number Packets (CSNPs) over a broadcast circuit. The CSNP contains the summary of all LSPs in the link state database. CSNPs are processed by the routers to ensure that their databases are synchronized. Because CSNPs must be processed by all routers, this interval should not be too short. However, setting this interval too long causes the router in the NLSP area to synchronize slowly when there are changes, such as routers going down.

- ◆ **Partial**—Time interval at which the router sends Partial Sequence Number Packets (PSNPs) on WAN circuits and request LSPs on LAN circuits. PSNPs are used to acknowledge LSPs.

◆ **Hello Intervals**—Hello packets used by NLSP to detect the presence of other NLSP nodes on the network. Three intervals are listed, all in seconds:

- ◆ **Broadcast**—Time interval at which NLSP Hello packets are sent on a broadcast circuit, such as Ethernet, token ring, or FDDI. The lower this value, the faster the network converges after a change in the network. The Maximum Age indicates how long the router considers another router active if it has not heard from the other router.

- ◆ **Non**-**Broadcast**—Time interval at which NLSP Hello packets are sent on a nonbroadcast circuit, such as WAN circuits. Setting this value too low causes frequent WAN traffic, which can be costly. The Maximum Age indicates how long the router considers another router active if it has not heard from the other router.

- ◆ **Designated Router Broadcas**t—Time interval at which the Designated Router sends NLSP Hello packets to LAN circuits. All systems in an NLSP area must have the same interval configured. Because the Designated Router is responsible for connectivity and synchronization on the LAN, this interval should be set to a low value. The Maximum Age indicates how long the router considers a Designated Router active if it has not heard from that router.

See your router documentation for more information about NLSP routers.

Viewing Router IPX Connections

The IPX Circuits table (Figure 10-9) gives you information about the IPX connections that the router has to LANs, WANs, and other IPX systems. To see the IPX Circuits table, double-click the Circuits icon in the IPX Router Details window, shown in Figure 10-6.

Figure 10-9
IPX Circuits Table

Name	Network Number	Status	Media Type	Interface Index	Circuit Type	Protocols	Bandwidth	Dela
NE3200_1_EII	69999172	Up	Ethernet II	3	Broadcast	NLSP	10m	
FDDI_1_FSP	61019000	Up	FDDI, SNAP	8	Broadcast	RIP	100m	
NE3200_3_E83	69999006	Up	IEEE 802.3	7	Broadcast	NLSP, RIP	10m	
NE3200_2_EII	69999002	Up	Ethernet II	1	Broadcast	RIP	10m	
NE2000_188_E82	61019188	Up	IEEE 802.3, IE	9	Broadcast	RIP	10m	

SJF-DEV - IPX Circuits

Table 10-4 explains the IPX Circuits table fields.

Table 10-4
IPX Circuits Table Fields

Field	Explanation
Name	Logical interface name, usually meaningful, assigned to the circuit by the system administrator when it was set up.
Network Number	Four-byte IPX network number assigned to the IPX network segment to which the circuit is connected.
Status	Indicates whether that circuit is functional and whether IPX Header Compression is enabled on the circuit.
Media Type	Media types on the circuit. For example, IEEE 802.3, 802.4, or 802.5; FDDI; Ethernet; ARCNET*, and so on.
Interface Index	Serial number assigned to the interface by the system. This number corresponds to the number shown in the Interface field in the Node Interfaces window. Use this number to correlate this logical circuit to the physical interface upon which the circuit is built. For WAN circuits, it is possible to see more than one circuit with the same Interface Index. This is because, for some WAN protocols (such as Frame Relay), multiple logical WAN circuits can be configured on a single physical connection.
Circuit Type	Circuit type, such as broadcast or point-to-point.
Protocols	Routing protocols enabled on the circuit. Different protocols can be enabled on different circuits. For example, for a given router, NLSP can be enabled on all WAN circuits while only RIP is enabled on the LAN circuits.
Bandwidth	Capacity of the circuit, measured in bits per second. The suffix of the bandwidth value is "K" or "M" to indicate kilobits or megabytes, respectively.
Delay	Estimated amount of time for a bit of data to reach the wire. This is in inverse proportion to the bandwidth; a high bandwidth suggests low delay, and low bandwidth suggests high delay. Delay is measured in microseconds.
Designated Router	Of the routers on the network segment, the one assigned to the circuit by NLSP. Displayed only if the router is running NLSP.

Viewing IPX Statistics for a Router

The IPX Statistics graph shown in Figure 10-10 gives you real-time information about the packets a router is receiving and transmitting. To see the IPX Statistics graph, double-click the Statistics icon in the IPX Router Details window.

Figure 10-10
IPX Statistics Graph
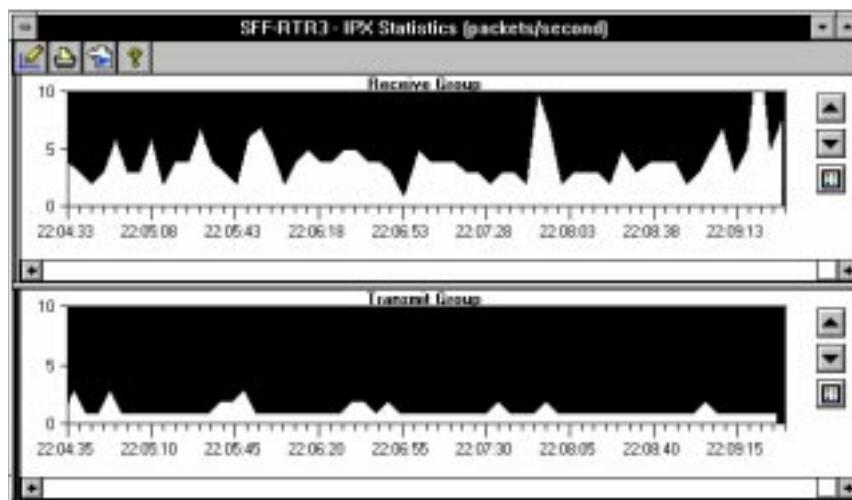
Below the action bar are two graphs: Receive Group and Transmit Group. The IPX Statistics graphs track the following statistics. You can click the Legend box to see the count of good and error packets and a breakdown of packet types. The following types of packets are counted:

◆ **Receive Group**—Shows the count for the following types of incoming packets:

  ◆ **To Be Forwarded**—Number of IPX packets this router is to forward because their destination is not this router.

  ◆ **Delivered**—Number of IPX packets that were delivered locally (within the router).

  ◆ **Filtered**—Number of incoming packets that were discarded because of filters set up by the system administrator.

- **Discarded**—Number of incoming packets this router discarded because of reasons other than packet header errors, unknown sockets, and decompression errors. The primary cause of packets being discarded is the router running out of buffers (which indicates a resource problem).

- **NETBIOS**—Number of NETBIOS packets received.

- **Error packets**—The following kinds of receive group error packets are counted:

  Header errors—Number of incoming IPX packets discarded due to errors in their headers.

  Unknown sockets—Number of incoming IPX packets discarded because the destination socket was not open.

  Bad checksums—Number of IPX packets received with incorrect checksums.

  Too many hops—Number of IPX packets discarded because they exceeded the maximum hop count configured on the router.

  Decompression errors—Number of IPX packets discarded due to decompression errors.

◆ **Transmit Group**—Shows the count for the following types of outgoing packets:

- **Transmitted**—Number of IPX packets leaving the router.

- **Filtered**—Number of outgoing IPX packets discarded due to filtering.

- **Discarded**—Number of outgoing IPX packets discarded due to reasons other than malformed requests, filtering, or compression errors. The primary cause of packets being discarded is the router running out of buffers, which indicates the router cannot handle the load.

- **Error packets**—The following kinds of transmit group error packets are counted:

  No router—Number of times the router did not have a route to a destination network.

  Malformed requests—Number of IPX packets generated locally within the router that had errors in their structure.

  Compression errors—Number of outgoing IPX packets discarded because of compression errors.

When the router is processing packets well, the peaks in the two graphs are much the same. If, for example, delivery of packets is high but forwarding of packets is low, the router is not routing many packets. A high delivery count might result from many management stations querying the router. The delivery count might also be high because a server is set up to be a router but the server does not have enough bandwidth to dedicate to routing. Most of a router's traffic should be dedicated to forwarding packets.

Suggestion If you create a baseline document of normal activity for a router, you can more easily distinguish between normal traffic and heavy traffic.

Errors are shown in red on the graph. You can click the graph at a point where red is shown, then click the Legend button. The Legend window appears, showing counts, by statistic, at that point in time. This information might help you determine the cause of the problem.

Monitoring NLSP Routers

ManageWise provides facilities for monitoring NLSP routers. You can display information about an NLSP area, save topology information to a file, and find the shortest paths between routers. These facilities are explained in the following sections.

About NLSP

NLSP is a link state routing protocol that supports hierarchical routing. At the lowest level of the hierarchy are the NLSP routing areas. An NLSP routing area is formed by a group of routers that uses the NLSP Level 1 routing protocol among themselves to communicate IPX routing information. Administratively, an NLSP routing area typically coincides with a subgroup within an organization.

Routers in an NLSP area communicate link state information among themselves. Each router keeps a link state database that records the routers and networks in an area and how they are connected. The database is used for making routing decisions. When the network is in a stable state, the link state database in each area router stays roughly the same.

NLSP management is centered around displaying the information in this link state database maintained by the routers.

Viewing NLSP Topology Information

To display NLSP topology information, follow these steps:

Procedure

1. **Display the global router summary by selecting** *View > All > Routers***.**

   The Router Summary table, Figure 10-1 on page 238, is displayed.

2. **Click the IPX Routers button in the action bar.**

   The IPX Routers window, Figure 10-4 on page 247, is displayed.

3. **Double-click any line in the IPX Routers window.**

   The IPX Router Details window, Figure 10-6 on page 250, is displayed.

4. **Double-click the NLSP Topology icon.**

   ManageWise queries the router for its link state database and the NLSP Topology window, Figure 10-11, is displayed.

Note   To view the IPX Router Details window for a non-routing NLSP server, select *File > Open > IPX Router*.

Figure 10-11
NLSP Topology Window
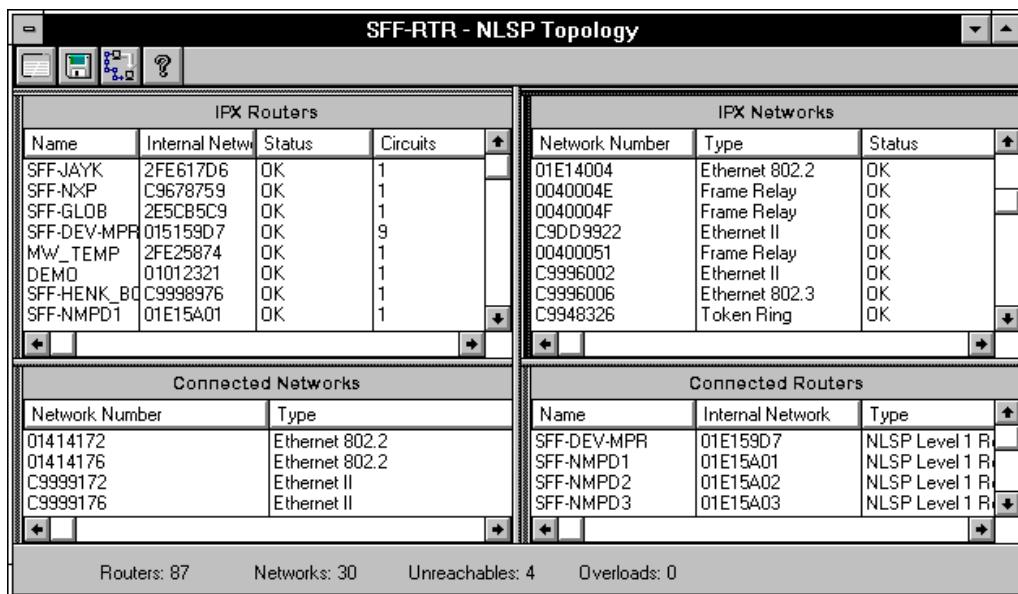
The body of the NLSP Topology window shows the view of the NLSP area from the perspective of the router selected in the IPX Router Details window.

The NLSP Topology window contains four window panes. When you select data in one of the top window panes, the window pane directly below it shows data that corresponds to your selection. ManageWise obtains data for this window dynamically. Therefore, if you want to save the NLSP topology shown, click the Save button and save the information in a file. The panes in the NLSP window contain the following data:

◆ **IPX Routers**—Shows the interconnected NLSP routers in the same NLSP area as the router selected in the IPX Router Details window (that is, it shows only the routers that use the NLSP protocol among themselves). When you select a router, the networks to which the router is connected are listed in the Connected Networks window pane below it. The IPX Routers window pane contains the following columns:

  ◆ **Name**—Name of the router.

  ◆ **Internal Network**—IPX internal network number of the router.

  ◆ **Status**—In typical conditions, shows a status of OK. In atypical conditions, the field might show a status of Unreachable, Overloaded, or Unreachable-Overloaded.

    Unreachable (in the case of NLSP routers) does not necessarily mean that the router is down. The router might be unreachable because it has been reconfigured with NLSP disabled and it takes time before the unreachable entries are deleted from the topology because of their age.

    If a router cannot store the topology because, for example, it has insufficient memory, the status indicates *Overloaded* until the router can store the NLSP topology again. NLSP routers do not try to route to other routers whose status is Overloaded.

  ◆ **Circuits**—Number of networks to which the router has connections. The number here corresponds to the number of networks listed in the Connected Networks window pane.

◆ **Connected Networks**—Shows data only if you select just one router in the IPX Routers window pane. This window pane shows all the networks to which the router selected in the IPX Routers window pane is connected. This window pane contains the following columns:

  ◆ **Network Number**—IPX network number assigned to the connection.

  ◆ **Type**—Type of network; for example, Ethernet II, token ring, FDDI.

- **IPX Networks**—Shows the interconnected IPX networks in the same NLSP area as the router selected in the IPX Router Details window. When you select a network in this window pane, the routers in that network are listed in the Connected Routers window pane below it. The IPX Networks window pane contains the following columns:

  - **Network Number**—Network number of the selected network.

  - **Type**—Type of network; for example, Ethernet II, token ring, FDDI.

  - **Status**—Shows a status of OK or Unreachable.

- **Connected Routers**—Shows all routers in the network selected in the IPX Networks window pane. This window pane contains the following columns:

  - **Name**—Name of the router.

  - **Internal Network**—IPX internal number of the router.

  - **Type**—NLSP level of the router, which is always NLSP Level 1 (until NetWare routers support NLSP Level 2).

Other ManageWise Commands for Managing Routers

You can also use the following ManageWise commands to monitor and manage the routers in your network:

- *Tools > SNMP MIB Browser*—Enables you to create profiles to monitor and manage routers using selected SNMP MIB variables. For further information about this command, refer to Chapter 12, "Managing SNMP Devices."

- *Tools > RCONSOLE*—Enables you to log in to the router and perform SUPERVISOR functions remotely. This is especially useful for NetWare routers to access configuration information. For further information about this command, refer to Appendix A, "Using Remote Console."

11 *Managing Hubs*

ManageWise® software can manage and monitor hubs that comply with the Novell® Hub Management Interface™ (HMI™) specification and that have the NetWare® Hub Services™ software installed on the server in which the hub is also installed.

Note ▼ No hub drivers compatible with the HMI specification are certified for NetWare 4.1. However, ManageWise manages hubs compatible with HMI on NetWare 3™ servers.

The NetWare Loadable Module™ (NLM™) files that make up NetWare Hub Services provide data to the ManageWise Console, which displays the data, manages the database and alarm monitoring systems, and provides maps of the networks.

ManageWise provides the following hub management data about all the HMI-compliant hubs on your network:

◆ **Configuration data**—Real-time data on the number of active ports, traffic volume for each hub, and the status of each hub in a hub server.

◆ **Traffic graphs**—Graphs displaying traffic volume for each hub and each port on the hub in a hub server.

◆ **Hub Statistics**—Detailed statistics about each hub.

◆ **Port Statistics**—Detailed statistics about all ports on all hubs.

Getting Started

Hub-related commands are integrated into the ManageWise menu.

You can perform all ManageWise operations, including hub management, by selecting menu commands or by selecting objects on maps or other windows.

You can use several methods to select and display the hub-related functions of a specific server containing HMI-compliant hubs:

◆ Display the All HMI Hubs window and select the HMI-compliant hub server by double-clicking the appropriate icon in the window.

◆ Enter the information in a dialog box to access that specific HMI-compliant hub server. This method requires that you know the name, IPX™ address, or IP address of the HMI-compliant hub server.

◆ Open a specific *managed* server that you know to contain a hub and, when the server configuration window is displayed, double-click the hub icon.

   Managed servers contain the NetWare Management Agent™ software; managed servers are indicated by the server icon with colored file folders.

◆ Double-click a hub icon in a segment map.

◆ Double-click a server on a segment map that contains a hub. Select the Hub:HMI icon from the Open Service dialog box.

Viewing All HMI Hubs

To locate HMI-compliant hubs on your network, select *View > All > HMI Hubs* to display the All HMI Hubs list, as shown in Figure 11-1.
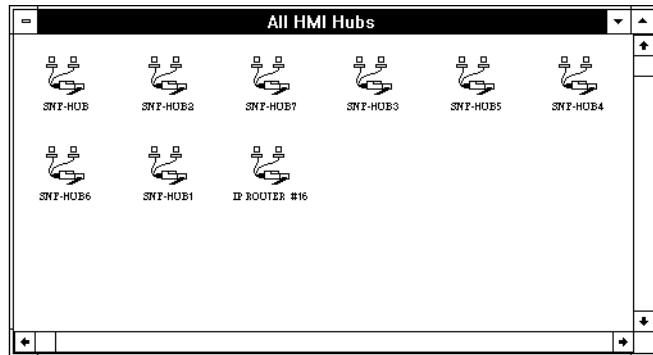
Note ▼ A new or modified hub server is shown on the All HMI Hubs list if the hub has sent SAP packets (and thus is listed in the local bindery), or the hub has been discovered by the NetExplorer™ software (and thus is in the database), or both.

Refer to *ManageWise 2.6 Setup Guide* for detailed information about how to use the discovery process to have new or modified hub configurations recognized.

To examine the details of a hub, double-click the icon of the hub you want to examine from the All HMI Hubs list. This brings up the Hub Backpanel window. For more information, refer to "Managing Hubs."

Selecting an HMI-Compliant Hub Server Directly

If you know the name, IPX address, or IP address of an HMI-compliant hub server, it might be quicker and more direct to select the server with the *File > Open > HMI Hub* command.

This command opens the Open HMI Hub dialog box, shown in Figure 11-2. You can enter either the hub name, IPX address, or IP address.

Select the way you are going to address the hub by clicking the option button next to the selection. After you select the form of address and enter it, click the Open button to bring up the hub display.
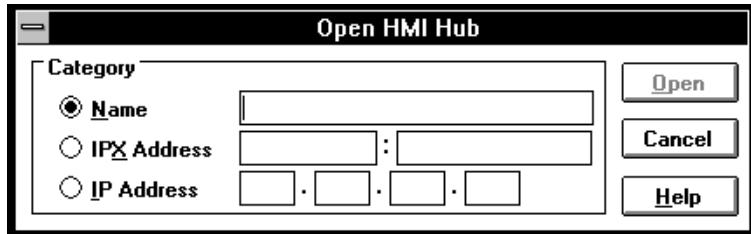
To open a hub *by name*, it must be in the database. You can open a hub by its IP address or its IPX address, though, even if it is not in the database (has not been discovered).

Managing Hubs

Hub information is displayed in the following two main windows, which use colors to indicate specific conditions for elements of a hub.

◆ Hub Backpanel window, which provides an overview of all hubs on the selected server and uses color codes to show the status of ports on the hubs.

A Custom Hub Backpanel window is displayed for any hub whose manufacturer has provided metafile support. Refer to documentation from that manufacturer for more information.

◆ Hub Port Map window, which displays detailed hub, card, and port configuration information and information about interconnection details for each hub, card, and port in the selected hub server.

From these two windows, you can display several other windows to view details about hubs, cards, and ports. From the ManageWise Performance menu, you can also view graphs displaying utilization for a selected hub, card, or port, and view tables of statistics.

Use these windows to isolate network troubles and to tune network operation.

Displaying Hub Information

The following sections describe how you can access hub information gathered by ManageWise.

Selecting the Hub Backpanel or Hub Port Map Window

The Hub Backpanel window provides an immediate overview of the condition of all ports on the selected hub server. You can display the Hub Backpanel window by double-clicking any of the hub server icons in the All HMI Hubs window, double-clicking a hub icon on the ManageWise maps, or double-clicking a hub icon in the NetWare Server Configuration window.

If you want more detailed information about the hub server, toggling to the Hub Port Map window gives you details about your hubs, including the object or segment connected to each port and the condition of each port.

Double-clicking the Hub Server icon for the SNF-HUB, selected from the All HMI Hubs list shown in Figure 11-1, displays the default Hub Backpanel window, shown in Figure 11-3. If metafile support for that hub was provided by the manufacturer, a Custom Hub Backpanel window is displayed.

Both the Hub Backpanel and Hub Port Map windows show a hub server configuration with hubs, cards in each hub, and ports on each card in each hub. The Hub Port Map window also shows the devices or services connected to each port, the state of the connection, and the ManageWise database name for each port. Figure 11-3 shows a Hub Backpanel window with two hubs containing two hub cards each. Figure 11-4 shows a sample Custom Hub Backpanel window.

Figure 11-5 shows a Hub Port Map window of the hub shown in Figure 11-3. These window options give you a choice between the Hub Backpanel window overview or the Hub Port Map window details. All data in these two windows is identical; the Hub Port Map window gives additional details about the objects connected to each port.

Figure 11-3
Hub Backpanel Window

Port Selection Buttons

Card Selection Buttons

Hub Selection Buttons
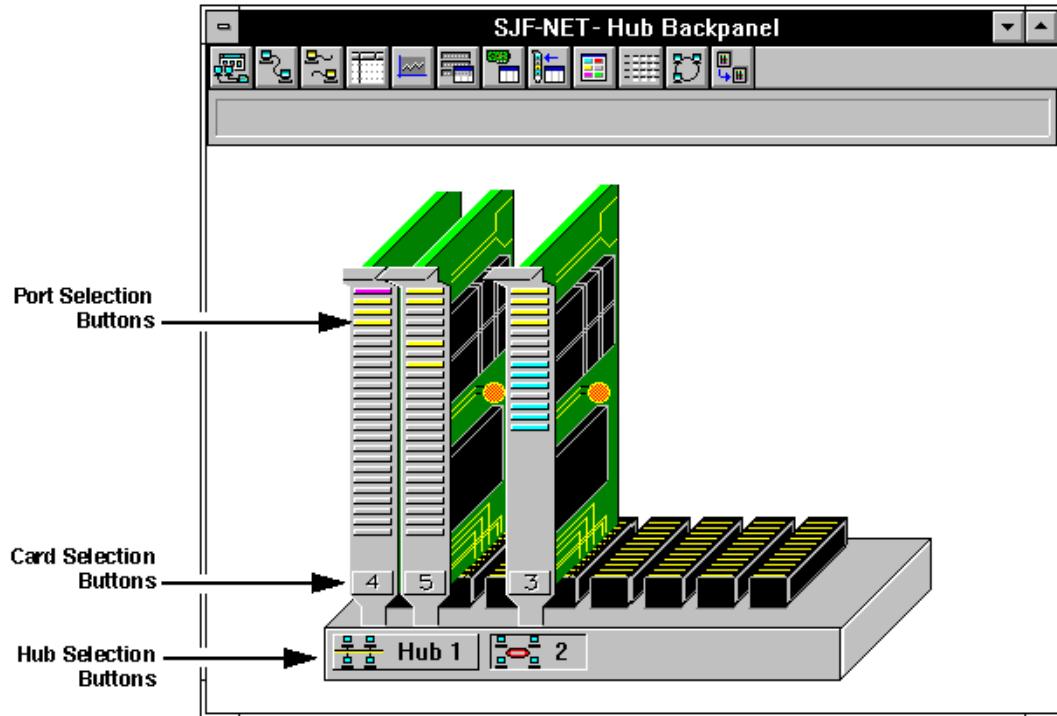
Hub Backpanel Window

The Hub Backpanel window gives an overall view of all hubs in a hub server, hub cards within each hub, and the ports on each hub card in a selected hub server. The port selection buttons are color-coded, giving an instant visual display of the condition of all ports in the hub server.

Custom Hub Backpanel Window

The Custom Hub Backpanel window provides a visual representation of a hub whose manufacturer has provided metafile support. A custom hub backpanel includes a view of all hub cards within the hub and the ports on each hub card. The port selection buttons and LEDs are color-coded, giving an instant visual display of the condition of all ports in

the hub server. In addition, access is provided to many of the hub management windows by double-clicking portions of the window. Figure 11-4 shows a Custom Hub Backpanel window.

Figure 11-4
Custom Hub Backpanel Window
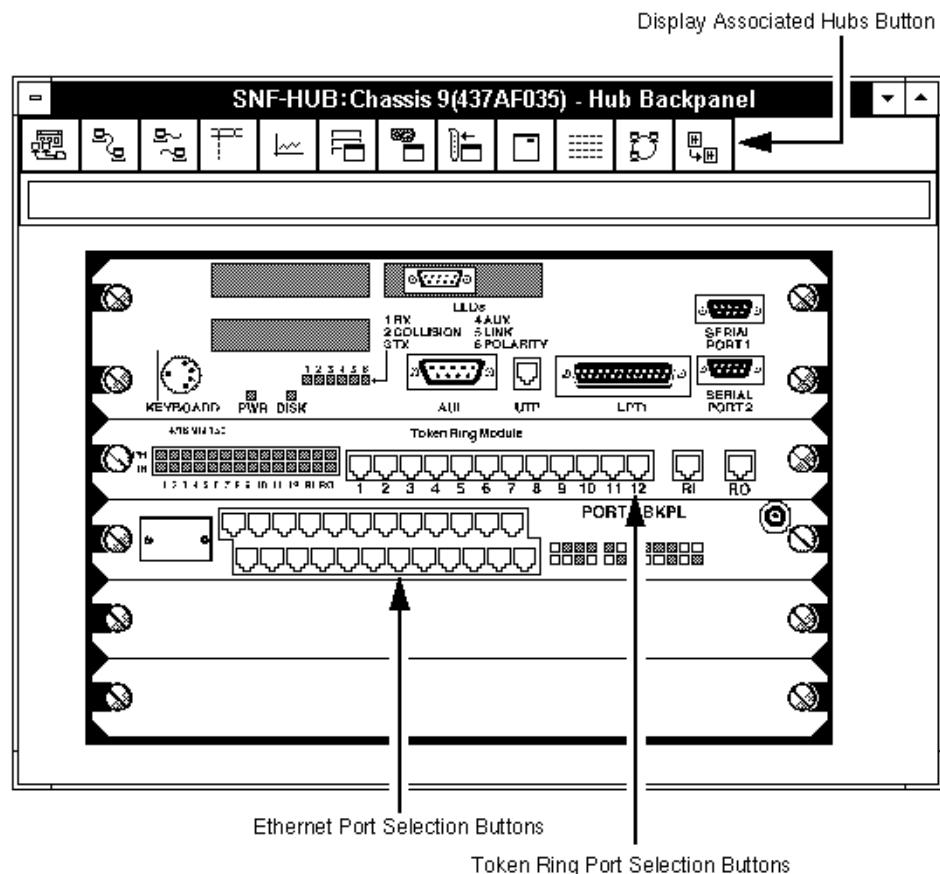
Individual hub ports and cards can be selected with a mouse. When selected, these ports and cards can be examined by selecting appropriate buttons from the action bar. Hubs, ports, and cards are selected as described:

◆ Clicking a port selects the individual port (Ethernet or token ring)

◆ Holding down Shift while clicking a port selects all ports on the same segment for Ethernet ports

◆ Holding down Shift while clicking a port selects all ports on the same ring for token ring ports

◆ Holding down Shift while clicking a card selects the hub

Additionally, a number of hub management windows, which are available elsewhere, can also be activated from the Custom Hub Backpanel window, as described in Table 11-1.

Table 11-1
Management Windows Activated from the Custom Hub Backpanel Window

Portion of Window Double-Clicked	Management Window Activated
Ports on Ethernet hub card	Double-clicking any of the ports on an Ethernet hub card brings up the Ethernet Hub Port Details window, as described in "Ethernet Hub Port Details Window" on page 278.
Ports on token ring hub card	Double-clicking any of the ports on a token ring hub card brings up the Token Ring Hub Port Details window, as described in "Token Ring Hub Port Details Window" on page 287.
Ethernet hub card	Double-clicking an Ethernet hub card brings up the Ethernet Hub Card Details window, as described in "Ethernet Hub Card Details Window" on page 277.
Token ring hub card	Double-clicking a token ring hub card brings up the Token Ring Hub Card Details window, as described in "Token Ring Hub Card Details Window" on page 286.
Anywhere on the chassis	Double-clicking the custom hub chassis anywhere when an Ethernet hub card or port is selected brings up the Ethernet Hub Details window, as described in "Ethernet Hub Details Window" on page 275. Double-clicking the custom hub chassis anywhere when a token ring hub card or port is selected brings up the Token Ring Hub Details window, as described in "Token Ring Hub Details Window" on page 282.

Portion of Window Double-Clicked	Management Window Activated
Designated hot spots	Any location on the hub cards or chassis designated by a manufacturer can be used to launch a management function. Refer to the documentation provided by the manufacturer of your hub hardware to determine whether there are locations other than those described in this table that, when double-clicked, provide access to management features.

Hub Port Map Window

The Hub Port Map window, Figure 11-5, displays the status of each port in a selected hub server. The Hub Port Map action bar buttons give you access to hub management windows. The following sections describe the functions and management information available from the Hub Port Map window.

Figure 11-5
Hub Port Map Window
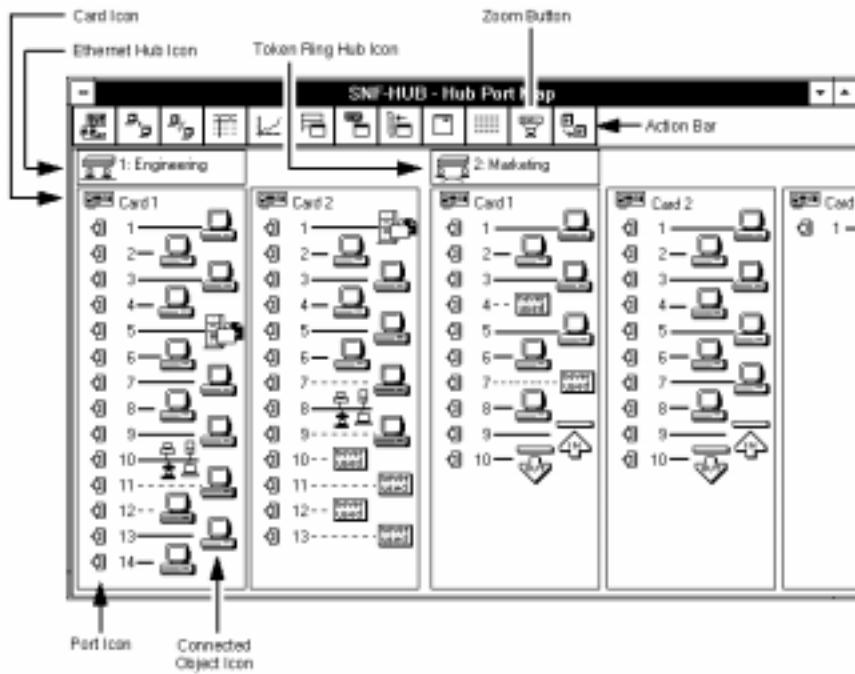
Hub Port Map Window Icon Details

The icons displayed for each port show the port status, the status of the connection, and the type of network object connected to the port.

Ethernet hub icon. Indicates that all the hub cards that appear under it are Ethernet hub cards. Double-clicking this icon brings up the Ethernet Hub Details window, shown in Figure 11-6.

Token ring hub icon. Indicates that all the hub cards that appear under it are token ring hub cards. Double-clicking this icon brings up the Token Ring Hub Details window, shown in Figure 11-9.

Card icon. Double-clicking the card icon displays detailed information about the status of the selected card, shown in Figure 11-7 and Figure 11-10.

Port icon. Double-clicking the port icon displays detailed information about the status of the selected port, shown in Figure 11-8 and Figure 11-11. In addition, the color of the port icon indicates the condition of the port.

The color codes for both the Hub Backpanel and Hub Port Map windows are as follows:

◆ **Cyan**—Indicates the port is operating normally.

◆ **Red**—Indicates there is an error on the port.

◆ **Yellow**—Indicates the port is disabled.

◆ **Violet**—Indicates the port is partitioned (Ethernet only).

◆ **Gray**—Indicates a link is down on the Hub Backpanel window.

Connection icon. Line connecting the port icon to the network object icon. It has the following states:

◆ **Dashed line**—Indicates no object is connected.

◆ **Thick solid line**—Indicates the port is connected to a PC or another network device.

Network object connected to the port icon. Displays either a Network Object Connected icon or a Never Used icon:

◆ **Network Object Connected icon.** Indicates the device or service that is or has been connected to the port.

◆ **Never Used icon.** Indicates no object has ever been connected to the port.

Ethernet Hub Details Window

To display the Ethernet Hub Details window, Figure 11-6, do one of the following:

◆ Double-click a hub icon in either the Hub Port Map or Hub Backpanel window.

◆ Click the Hub Statistics button on the action bar.

◆ Select a hub icon, and then select *File > Open > Selected Object.*

Figure 11-6
Ethernet Hub
Details Window
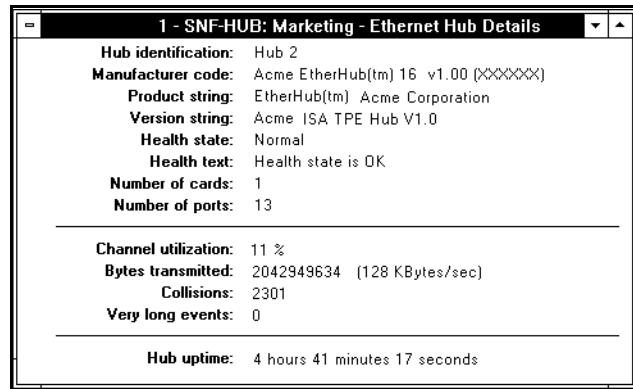
1 - SNF-HUB: Marketing - Ethernet Hub Details

Hub identification:	Hub 2
Manufacturer code:	Acme EtherHub(tm) 16 v1.00 (XXXXXX)
Product string:	EtherHub(tm) Acme Corporation
Version string:	Acme ISA TPE Hub V1.0
Health state:	Normal
Health text:	Health state is OK
Number of cards:	1
Number of ports:	13
Channel utilization:	11 %
Bytes transmitted:	2042949634 (128 KBytes/sec)
Collisions:	2301
Very long events:	0
Hub uptime:	4 hours 41 minutes 17 seconds

The Ethernet Hub Details window contains the following information:

Hub identification—Hub number, as shown on the Hub Port Map and Hub Backpanel windows.

Manufacturer code—By default, a numeric code assigned to the hub card by the manufacturer. Figure 11-6 shows a numeric code translated to a text string. You can configure your installation to perform this translation by modifying the HSM.INI file in your Windows directory. For your convenience, common hub vendors are already listed at the end of the HSM.INI file.

Product string—Manufacturer's product name for the hub.

Version string—Hub version.

Health state—Operating condition of the card. If the status of the card is impaired for any reason, this field flags the condition.

Health text—Text string describing the condition of the hub, as described under Health state.

Number of cards—Number of cards in this hub.

Number of ports—Number of ports reported by the cards in the hub, including AUI and local host ports on some card types. The number of ports might not match the number of physical 10BASE-T ports. One reason the numbers might not match is because the local host port, if any, is a logical port; it might not be a physical 10BASE-T port.

Channel utilization—Percentage of the channel capacity currently being used by all the combined ports on the hub, by hub.

Bytes transmitted—Number of bytes transmitted and number of kilobytes per second transmitted on this hub.

Collisions—Number of packet collisions detected.

Very long events—Number of times the card has detected very long events.

Hub uptime—Length of time the server has been up.

Note ▼ Because it is possible to remove some hub cards without turning off the server, it is possible to remove or replace hubs without affecting the cumulative hub uptime reported.

Ethernet Hub Card Details Window

The Ethernet Hub Card Details window, Figure 11-7, is displayed when you do one of the following:

◆ Double-click a card icon for an Ethernet card on the Hub Port Map window or on the Hub Backpanel window.

◆ Select a card icon for an Ethernet card on the Hub Port Map window or Hub Backpanel window and then click the action bar icon to display the Ethernet Hub Card Details window.

◆ Select a card icon for an Ethernet card on the Hub Port Map window or Hub Backpanel window and then select *File > Open > Selected Object.*

Figure 11-7
Ethernet Hub Card
Details Window
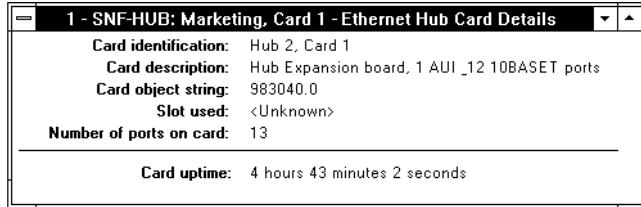
```
┌─────────────────────────────────────────────────────────────┐
│ ▬    1 - SNF-HUB: Marketing, Card 1 - Ethernet Hub Card Details  ▼ ▲ │
├─────────────────────────────────────────────────────────────┤
│         Card identification:  Hub 2, Card 1                    │
│          Card description:  Hub Expansion board, 1 AUI _12 10BASET ports │
│         Card object string:  983040.0                          │
│               Slot used:  <Unknown>                            │
│     Number of ports on card:  13                               │
│  ─────────────────────────────────────────────────────────── │
│             Card uptime:  4 hours 43 minutes 2 seconds         │
└─────────────────────────────────────────────────────────────┘
```

The Ethernet Hub Card Details window contains the following information:

Card identification—Hub and card number, as shown on the Hub Backpanel and Hub Port Map windows.

Card description—Card description supplied by the card manufacturer.

Card object string—Object ID supplied by the card manufacturer.

Slot used—Slot occupied by the card (servers with an EISA bus motherboard, for example), or displays <Unknown> (for other motherboard bus configurations, such as ISA).

Number of ports on card—Number of ports reported by the card, including AUI and local host ports on some card types. The number of ports might not match the number of physical 10BASE-T ports. One

reason the numbers might not match is because the local host port, if any, is a logical port; it might not be a physical 10BASE-T port.

Card uptime—Length of time since the server was most recently brought up.

Note Because it is possible to remove some hub cards without turning off the server, it is possible to remove or replace hub cards without affecting the cumulative hub card uptime reported.

Ethernet Hub Port Details Window

The Ethernet Hub Port Details window, Figure 11-8, is displayed when you do one of the following:

◆ Double-click an Ethernet port icon on either the Hub Port Map or Hub Backpanel window.

◆ Click the Port Statistics button when an Ethernet port is selected.

◆ Select an Ethernet port and then select *File > Open > Selected Object.*

◆ From the Statistics table, double-click a row.

Figure 11-8
Ethernet Hub Port Details Window

Window title: 2 - SNF-HUB: Marketing, Card 1, Port 2 - Hub Port Details

Port identification: Hub 1, Card 1, Port 1, Segment 1
Logged-in user name: <None>
Port status: Enabled   Link up   Not partitioned
Channel utilization: 12 %
Readable frames: 9877943   (583 Frames/sec)
Bytes: 1961946806   (145 KBytes/sec)
Last MAC address: 00-00-1B-31-C0-7F
MAC address changes: 9248647

Total errors: 186 (1 Errors/sec)
Collisions: 9205
Late events: 6
FCS errors: 54
Alignment errors: 132
Frames too long: 0
Runts: 0
Very long events: 0
Short events: 0
Data rate mismatches: 0
Auto-partitions: 0

Utilization: KBytes/sec
200
160
120
80
40
0
15:31:51 15:33:21 15:34:51 15:36:21

Port uptime: 4 hours 53 minutes 33 seconds

Ethernet Hub Port Details Window Icon Details

The Ethernet Hub Port Details window icon displays either a Network Object Connected icon or a Never Used icon:

◆ **Network Object Connected icon.** Indicates the device or service is or has been connected to the port.

◆ **Never Used icon.** Indicates no object has ever been connected to the port.

Information Displayed in Ethernet Hub Port Details Window

The Ethernet Hub Port Details window shows operating details for the selected port. The information displayed in the Ethernet Hub Port Details window is as follows:

Port identification—Hub number, card number, port number, and segment value for the port, as displayed on the Hub Port Map and Hub Backpanel windows.

Logged-in user name—Username of the current client logged in to the port is displayed, if available.

Port status—Whether the port is enabled or disabled, whether the link is up or down, and whether the port has been partitioned.

Channel utilization—Real-time utilization of the port in percentage of port capacity.

Readable frames—Total number of readable frames received by the port and the current rate in frames per second.

Bytes—Total number of bytes passed by the port and also the current rate of traffic through the port in kilobytes per second.

Last MAC address—Current Media Access Control (MAC) address for the port. The MAC address is updated by the address from the last transmitted packet on the port.

MAC address changes—Total number of MAC address changes for the port. If this port attaches to another segment, this number is usually large.

Total errors—Total number of errors and the current error rate in errors per second on the port being examined. This number is the sum of all the following errors: late events, FCS errors, alignment errors, frames too long, runts, very long events, short events, and data rate mismatches.

Collisions—Number of collisions detected by the port. Collisions are a normal event on an Ethernet network. They occur when two or more nodes attempt to transmit simultaneously. A large number of collisions usually indicates a high load on the network, but can also be caused by a network adapter board failure.

Late events—Number of late collisions or events detected at the port. A late event is a collision that occurs later in the transmission than should be possible, if the basic networking rules (protocols) are followed. Because stations listen for traffic before transmitting, collisions should occur only when two or more stations transmit nearly simultaneously, resulting in a collision early in the transmission. A late collision indicates a faulty network controller or a violation of the rules of topology: network too big, too many repeaters connected in a series, and so forth.

FCS errors—Number of Frame Check Sequence (FCS) errors detected at the port. An FCS is appended to all packets to guard against errors. An FCS error occurs when a packet is involved in a collision, when it has been corrupted by noise, or when an error in the sending network controller occurs (such as transmit FIFO underrun).

Alignment errors—Number of alignment errors detected at the port. An alignment error indicates that a packet was received that could not be framed properly. Therefore, the contents of the packet could not be interpreted properly and were rejected. These malformed packets might be the result of collisions, noise, or hardware failures.

Frames too long—Number of long frames detected at the port. These frames are longer than the maximum length of a well-formed Ethernet frame, but not as long as frames that result from a transmitter that is stuck "on" and transmitting continuously (jabbering).

Runts—Number of runts detected at the port. A runt is a small packet received with FCS or alignment errors. It is the result of collisions occurring on a connected segment or between stations connected to attached repeaters. Runts are essentially "inferred collisions." Collisions between ports within the same repeater are detected

explicitly. Runts are artifacts of collisions that cannot be detected explicitly because they are somewhat remote to the repeater observing the runt.

Very long events—Number of long events detected at the port. A very long event is presumed to be caused by continuously transmitting (jabbering) nodes. The repeater does not repeat the full length of such an event because it would cause faulty operation of certain network elements.

Short events—Number of short events detected at the port. A short event is not an actual packet, but it occurs when noise causes the repeater to initiate its normal packet repeat process. It is detected as a short event by virtue of being shorter than the shortest possible collision fragment.

Data rate mismatches—Number of data rate mismatches detected at the port. A data rate mismatch indicates that a significant difference in frequency exists between the clocks in the sending and receiving stations. A port reporting a data rate mismatch is usually connected to a faulty station. If all (or a number of) ports report a data rate mismatch, the hub network controller contains a faulty clock source.

Auto-partitions—Number of times the port has been autopartitioned. Autopartitioning is a mechanism by which a repeater isolates a malfunctioning station or segment of the network from other functioning segments. A station or segment is partitioned automatically if it is the source of a large number of consecutive collisions or the source of abnormally long collisions. The segment remains partitioned as long as the condition persists.

Port uptime—Length of time since the server was most recently brought up.

Note ▼ Because it is possible to remove some hub cards without turning off the server, it is possible to remove or replace hub cards without affecting the cumulative port uptime reported.

Ethernet Hub Port Utilization

The Ethernet Hub Port Details window includes a small graph of Ethernet hub port utilization as either a percentage of the port capacity or as the number of kilobytes per second currently handled by the port.

The control buttons (vertical axis scale, number, and percentage) operate the same as those on the Hub Port Utilization Graph. For more information, refer to the online help.

Enable and Disable Buttons

The Ethernet Hub Port Details window provides buttons for you to enable or disable the port being displayed. This tool gives you the ability to control and configure the network to isolate problems.

Token Ring Hub Details Window

To display the Token Ring Hub Details window, Figure 11-9, do one of the following:

◆ Double-click a token ring hub icon in either the Hub Port Map or Hub Backpanel window.

◆ Click the Hub Statistics button on the action bar.

◆ Select a hub icon and then select *File > Open > Selected Object.*

Figure 11-9
Token Ring Hub
Details Window

```
┌─────────────────────────────────────────────────────────────────┐
│ ─          SNF-HUB: bar - Token Ring Hub Details            ▼ ▲ │
├─────────────────────────────────────────────────────────────────┤
│          Hub identification:  Hub 2                               │
│         Manufacturer code:  Acme TokenHub(tm) v1.00 (XXXXXX)      │
│              Product string:  TokenHub(tm) Acme Corporation       │
│              Version string:  Acme Token Hub v1.0                 │
│               Health state:  Normal                               │
│                Health text:  Hub is OK                            │
│            Number of cards:  2              Number of ports:  15  │
│          Concentrator type:  Retiming    Concentrator speed:  4 Mbs│
│             Active monitor:  10-00-5A-E1-04-77                    │
│            Monitor changes:  1                                    │
│   ─────────────────────────────────────────────────────────────  │
│                  Total errors:   6  ( 0 Errors/sec)               │
│             Monitor errors:  0      Beacon (set recovery):  0     │
│           Frequency errors:  0        Beacon (signal loss):  0    │
│                Lost frames:  3         Beacon (streaming):  0     │
│         Receive congestions:  0         Duplicate monitors:  0    │
│          Frame copied errors:  0        Duplicate addresses:  0   │
│                Token errors:  3            Ring poll failures:  0  │
│   ─────────────────────────────────────────────────────────────  │
│               Hub uptime:  12 minutes 18 seconds                  │
└─────────────────────────────────────────────────────────────────┘
```

The Token Ring Hub Details window contains the following information:

Hub identification—Hub number, as shown on the Hub Port Map and Hub Backpanel windows.

Manufacturer code—By default, a numeric code assigned to the hub card by the manufacturer. Figure 11-9 shows a numeric code translated to a text string. You can configure your installation to perform this translation by modifying the HSM.INI file in your Windows directory. For your convenience, common hub vendors are already listed at the end of the HSM.INI file.

Product string—Manufacturer's product name for the hub.

Version string—Hub version.

Health state—Operating condition of the card. If the status of the card is impaired for any reason, this field flags the condition.

Health text—Text string describing the condition of the hub, as described under Health state.

Number of cards—Number of cards in this hub.

Number of ports—Number of ports reported by the cards in the hub, including local host ports on some card types. The number of ports might not match the number of physical token ring ports. One reason the numbers might not match is because the local host port, if any, might not be a physical token ring port.

Concentrator type—Status of the concentrator as Retiming, Non-retiming, or Other.

Concentrator speed—Speed, in megabits per second, of the token ring supported by the hub.

Active monitor—MAC address of the current active monitor.

Monitor changes—Number of times the active monitor has changed since the hub was brought up.

Total errors—Total number of errors and the error rate (in errors per second) on the port being examined. This number is the sum of all the following errors: monitor errors, frequency errors, lost frames, receive congestions, frame copied errors, token errors, beacon (set recovery), beacon (signal loss), beacon (streaming), duplicate monitors, duplicate addresses, and ring poll failures.

Monitor errors—Total number of soft errors and beacon errors reported by this hub. Soft errors are intermittent errors that the ring can generally recover from without disrupting ring functionality. Beacon errors, however, might require manual intervention if the ring cannot recover automatically.

Frequency errors—Number of errors indicating that the frequency of the incoming signal differs from the station's crystal oscillator by more that 0.6%.

Lost frames—Number of lost frames detected. When a ring station transmits the physical trailer of a frame, it starts a timer. If it has not stripped the same trailer off before the timer expires, it increments its Lost Frame counter and reports the error.

Receive congestions—Number of times a ring station detects a frame addressed to its specific address but has insufficient buffer space to copy it. This indicates that the station is congested.

Frame copied errors—Number of frame copied errors that have occurred on the ring. A frame copied error occurs when a station detects a frame addressed to its specific address and when bits are set that indicate another station either copied the frame or recognized the address. This indicates either a duplicate address on the ring or line noise.

Token errors—Number of token errors that have occurred on the ring. A token error occurs when the token gets corrupted or when the active monitor doesn't see any new frames transmitted in the required amount of time.

Beacon (set recovery)—Number of Claim Token MAC frames received or transmitted on the hub after the repeater has received a Ring Purge MAC frame. This counter signifies the number of times the ring has been purged and is set to recover to a normal operating state.

Beacon (signal loss)—Number of times the repeater has detected a signal loss from the ring. This condition is usually the result of a broken ring, faulty wiring at the concentrator end, transmitter malfunction, or receiver malfunction.

Beacon (streaming)—A combination of counters: bit streaming and frame streaming. The bit streaming counter removes (destroys) tokens and frames by writing over (repeat and transmit both occurring) or replacing (uncontrolled transmit) ring data. This process initiates monitor contention. Frame streaming is continuous transmission of tokens, abort sequences, or frames.

Duplicate monitors—Number of times more than one active monitor is detected on the ring.

Duplicate addresses—Number of times a duplicate MAC address was detected on the ring.

Ring poll failures—Number of times a station on the ring has failed in the process of polling for the address of its nearest active upstream neighbor.

Hub uptime—Length of time the server has been up.

Note   Because it is possible to remove some hub cards without turning off the server, it is possible to remove or replace hub cards without affecting the cumulative hub uptime reported.

Token Ring Hub Card Details Window

To display the Token Ring Hub Card Details window, Figure 11-10, do one of the following:

◆ Double-click a card icon from a Hub Port map or Hub Backpanel window.

◆ Click a token ring card to select it, and then click the Card Statistics button on the action bar

◆ Click a token ring card to select it, and then select *File > Open > Selected Object.*

Figure 11-10
Token Ring Hub Card Details Window
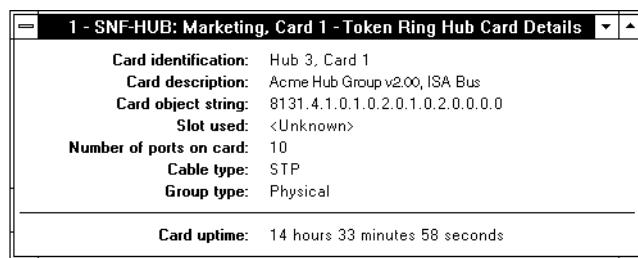
The Token Ring Hub Card Details window contains the following information:

Card identification—Hub and card number, as shown on the Hub Backpanel and Hub Port Map windows.

Card description—Card description supplied by the card manufacturer.

Card object string—Object ID supplied by the card manufacturer.

Slot used—Slot occupied by the card (for servers with an EISA bus motherboard for example) or displays <Unknown> (for other motherboard bus configurations, such as ISA).

Number of ports on card—Number of ports reported by the cards in the hub, including local host ports on some card types. The number of ports might not match the number of physical token ring ports. One reason the numbers might not match is because the local host port, if any, might not be a physical token ring port.

Cable type—Type of cable used for connecting the ports to the stations: shielded twisted pair, unshielded twisted pair, fiber, or other.

Group type—Type of group: either physical or external.

Card uptime—Length of time since the server was most recently brought up.

Note ▼ Because it is possible to remove some hub card types without turning off the server, it is possible to remove or replace hub cards without affecting the cumulative hub card uptime reported.

Token Ring Hub Port Details Window

The Token Ring Hub Port Details window, Figure 11-11, is displayed when you do one of the following:

◆ Double-click a token ring port icon on either the Hub Backpanel or Hub Port Map window or Token Ring map.

◆ Click the Port Statistics button when a token ring port is selected.

Figure 11-11
Token Ring
Hub Port
Details Window

```
┌─────────────────────────────────────────────────────────────────┐
│ ▭   2 - SNF-HUB: Marketing, Card 1, Port 2 - Token Ring Hub Port Details  ▼ ▲│
├─────────────────────────────────────────────────────────────────┤
│       Port identification:  Hub 2, Card 1, Port 2          ┌───────┐│
│      Logged-in user name:  <None>                          │ Enable ││
│            Port status:  Enabled   Inserted   Normal       └───────┘│
│         Last MAC address:  00-00-F6-09-39-0F               ┌───────┐│
│      MAC address changes:  1                               │Disable ││
│               Neighbor:  10-00-28-66-68-A1                 └───────┘│
│        Neighbor changes:  1                                 ┌────┐  │
│       Functional address:  Not Enabled                     │ 💻 │  │
│                                                             └────┘  │
│                   Total errors: 0  ( 0 Errors/sec)                 │
│         Line errors:  0            Duplicate addresses:  0         │
│        Burst errors:  0            Receive congestions:  0         │
│           AC errors:  0          Beacon (set recovery):  0         │
│    Abort transmissions:  0         Beacon (signal loss):  0        │
│       Internal errors:  0           Beacon (streaming):  0         │
│                                                                     │
│        Port uptime:  4 hours 53 minutes 33 seconds                 │
└─────────────────────────────────────────────────────────────────┘
```

Token Ring Hub Port Details Window Icon Details

The Token Ring Hub Port Details window icon displays either a
Network Object Connected icon or a Never Used icon:

◆ **Network Object Connected icon.** Indicates the device or service
that is or has been connected to the port.

◆ **Never Used icon.** Indicates no object has ever been connected to the
port.

Information Displayed in Token Ring Hub Port Details Window

The Token Ring Hub Port Details window shows operating details for
the selected port. The information displayed in the Token Ring Hub
Port Details window is as follows:

Port identification—Hub, card, and port number for the port, as
displayed on the Hub Backpanel and Hub Port Map windows.

Logged-in user name—Username of the current client logged in to the
port is displayed, if available.

Port status—Whether the port is enabled or disabled, whether the link
is inserted or not inserted, and the port type.

Last MAC address—Last MAC address observed on the port.

MAC address changes—Number of times the last address changed
since the hub was most recently brought up.

Neighbor—Physical (MAC) address of the downstream station relative
to this port.

Neighbor changes—Number of times the downstream neighbor for
this port has changed since the hub was most recently brought up.

Functional address—Group address of the port that provides a well-
known address for network functions such as active monitor, ring error
monitor, and so on.

Total Errors—Total number of errors and the error rate (in errors per second) on the port being examined. This number is the sum of all the following errors: line errors, burst errors, AC errors, abort transmissions, internal errors, duplicate addresses, receive congestions, beacon (set recovery), beacon (signal loss), and beacon (streaming).

Line errors—Number of times a frame or token is copied or repeated by a station. More specifically, this error occurs when the following criteria are met: the Error Detected Indicator (E) bit is zero in the incoming frame and one of the following conditions exists:

◆ A non-data bit lies between the Start Delimiter and the End Delimiter of the frame or token.

◆ An FCS error is in the frame.

Burst errors—Number of times a station detects the absence of transitions for five half-bit times (burst-five errors).

AC errors—Number of times a station receives an Active Monitor Present (AMP) or Standby Monitor Present (SMP) frame in which the AC bits are equal to zero.

Abort transmissions—Number of times a station transmits an abort delimiter during transmission.

Internal errors—Number of times a station recognizes an internal error.

Duplicate addresses—Number of times a duplicated address is detected on the ring.

Receive congestions—Number of times a ring station detects a frame addressed to its specific address but has insufficient buffer space to copy it. This indicates that the station is congested.

Beacon (set recovery)—Number of Claim Token MAC frames received or transmitted on the port after the repeater has received a Ring Purge MAC frame. This counter signifies the number of times the ring has been purged and is set to recover to a normal operating state

Beacon (signal loss)—Number of times the repeater has detected a signal loss from the port. This condition is usually the result of a broken ring, faulty wiring at the concentrator end, transmitter malfunction, or receiver malfunction.

Beacon (streaming)—Combination of counters: bit streaming and frame streaming. The bit streaming counter removes (destroys) tokens and frames by writing over (repeat and transmit both occurring) or replacing (uncontrolled transmit) ring data. This process initiates monitor contention. Frame streaming is continuous transmission of tokens, abort sequences, or frames.

Port uptime—Length of time since the server was most recently brought up.

Note ▼ Because it is possible to remove some hub card types without turning off the server, it is possible to remove or replace hub cards without affecting the cumulative port uptime reported.

Enable and Disable Buttons

The Token Ring Hub Port Details window provides buttons for you to enable or disable the port being displayed. This tool gives you the ability to control and configure the network to isolate problems.

Ring In/Ring Out or Daisy In/Daisy Out Hub Port Details Window

The Ring In/Ring Out (or Daisy In/Daisy Out) Hub Port Details window, Figure 11-12, is displayed when you do the following:

◆ Double-click a token ring port icon for the ring in/ring out (or daisy in/daisy out) ports on a token ring hub on either the Hub Backpanel or Hub Port Map window.

◆ Click the Port Statistics button when a ring in/ring out (or daisy in/daisy out) port is selected.

◆ Select *File > Open > Selected Object* when a ring in/ring out (or daisy in/daisy out) port is selected.

**Figure 11-12
Ring In/Ring Out
(Daisy In/Daisy Out)
Hub Port Details
Window**
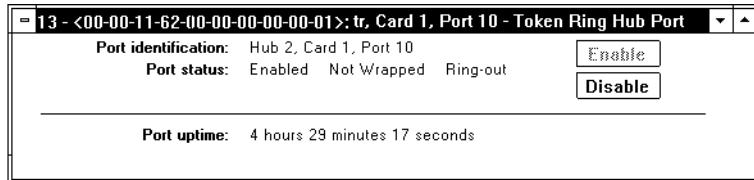
This window shows operating details for the selected port. The information displayed in the Token Ring Hub Port Details window is as follows:

Port identification—Hub, card, and port number for the port, as displayed on the Hub Backpanel and Hub Port Map windows.

Port status—Whether the port is enabled or disabled, whether the link is wrapped or not wrapped, and what type of port it is. The type of port can be either ring in, ring out, daisy in, or daisy out.

Port uptime—Length of time since the server was most recently brought up.

Note Because it is possible to remove some hub card types without turning off the server, it is possible to remove or replace hub cards without affecting the cumulative port uptime reported.

Enable and Disable Buttons

The Ring In/Ring Out Hub Port Details window and Daisy In/Daisy Out Port Details window provide buttons for you to enable or disable the port being displayed. This tool gives you the ability to control and configure the network to isolate problems.

Token Ring Map Window

The Token Ring Map window gives a graphic view of the logical ring containing the stations connected to ports on the selected token ring hub. This window provides a dynamic view of ring station status. It also provides access to all ManageWise controls and statistics for the token ring hub, ports, and stations.

To display the Token Ring Map window, Figure 11-13, select a hub, card, or port for a token ring hub and click the Token Ring Map button on the Hub Backpanel or Hub Port Map window.

Figure 11-13
Token Ring Map
Window
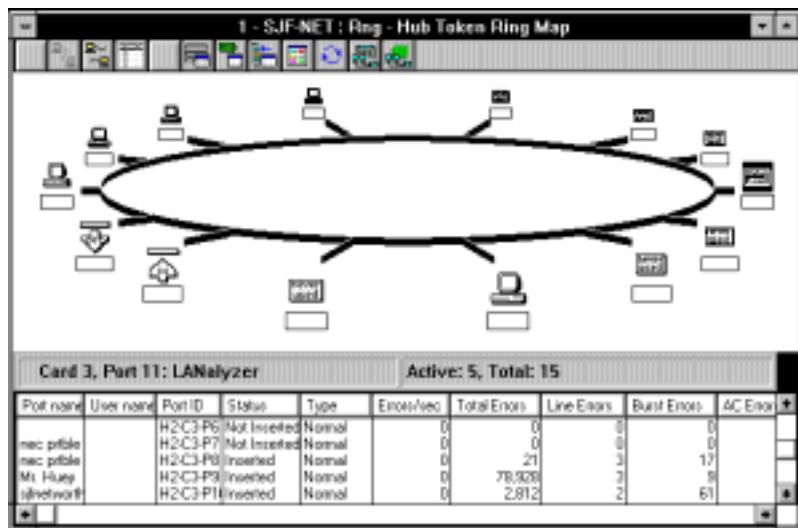
If the ring appears broken at the top of the window, there are more
stations on the ring than there is space to display them in the window.
You can change the view of the ring and bring currently hidden stations
into view by selecting a station with your left mouse button and
dragging it to any other location on the ring. This causes the ring to
rotate the display of the stations.

Token Ring Map Window Icon Details

In the Token Ring Map window, the icons displayed for each token ring
port on the logical ring show the port status, the position on the ring,
and the type of port.

◆ **Network Object Connected icon.** Indicates the device or service
that is or has been connected to the port.

◆ **Never Used icon.** Indicates no object has ever been connected to the
port.

◆ **Ring In and Ring Out icons.** Display the Ring In/Ring Out and the
Daisy In/Daisy Out ports of the hub card. Double-clicking the
Status button below these icons brings up the Ring In/Ring Out
Hub Port Details window or the Daisy In/Daisy Out Hub Port
Details window, as described in Figure 11-12 on page 290.

◆ **Status button**. Displayed under each Network Object Connected and Ring In/Ring Out (or Daisy In/Daisy Out) icon on the logical ring. The color of the Status button indicates the condition of the port:

  ◆ **Cyan**—Indicates the port is operating normally.

  ◆ **Red**—Indicates there is an error on the port.

  ◆ **Yellow**—Indicates the port is disabled.

  ◆ **Gray**—Indicates a link is down.

Error Domains. If an error is detected on a station, the likely domain of the error is highlighted in red on the ring. In most cases, this is the area on the ring between the reporting station and its upstream neighbor.

Figure 11-14 shows a a typical error domain between two stations. If Station A is reporting an error, the portion of the ring from Station A to Station B is highlighted in red. This is because the token moves clockwise in this window and Station B is the upstream neighbor of Station A.

Figure 11-14
A Token Ring Station and Its Upstream Neighbor
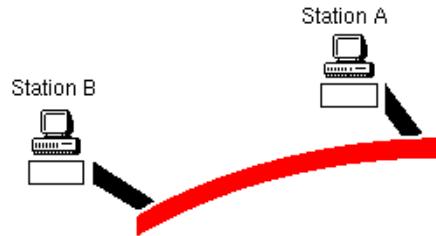
Testing Hubs

To test a hub, first select the hub to be tested by clicking the hub icon on either the Hub Backpanel or Hub Port Map window. Select the test procedure with the *Fault > Test Hub* command from the ManageWise menu bar. The Hub Fault Test dialog box, Figure 11-15, is displayed.

**Figure 11-15
Hub Fault Test
Dialog Box**
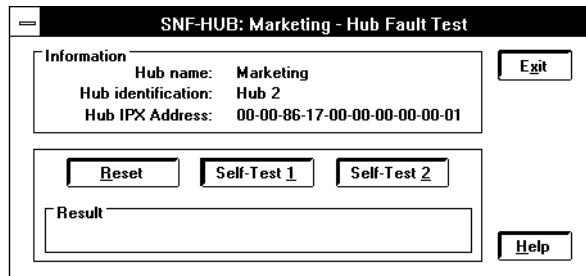
You can perform three actions with the capabilities built into hubs that conform to the Novell HMI standard:

◆ Hub Hardware Reset

◆ Self-Test 1

◆ Self-Test 2

Hub Hardware Reset

To reset a hub, click the Reset button shown in Figure 11-15. This initiates a *hub hardware* reset for the selected hub and reports that the hardware has been reset. Resetting the hub resets the hub hardware and puts it into a known state, as defined by the hardware manufacturer.

Note ▼ Resetting the hub does not reset ManageWise. The reset does not affect the configuration, port names, or hub names you have entered, or any data stored in the ManageWise database. It does not inject any packets on the network and does not add to the network load.

Self-Tests

You can use either Self-Test 1 or Self-Test 2 to check the operating status of any HMI-compliant hub on your network.

After completing the test, the hub reports the test results to ManageWise.

Note ▼ The test sequence and the board parameters tested for both Self-Test 1 and Self-Test 2 are determined by the hub card manufacturer.

Self-Test 1 and Self-Test 2 might not perform identical tests on a hub card, and might not give identical results even when run on the same card. Check the manual supplied with your hub card for details about what tests are actually performed for both Self-Test 1 and Self-Test 2.

Self-Test 1

Self-Test 1 is a nondisruptive test that does not interfere with packet relay. On some hub cards, this test might take longer than Self-Test 2, particularly on hub cards with high traffic volume. Other hub cards might give an almost immediate result, if no test is performed.

Note ▼ This test does not affect ManageWise configuration data, port names, or hub names you have entered. This test does not inject any packets on the network and does not add to the network load.

To run Self-Test 1, click the Self-Test 1 button.

Self-Test 2

Self-Test 2 does not apply to token ring hubs. Where it is used, it might interfere with packet relay; that is, packets received while this test is being performed might not be relayed. ManageWise recognizes the potential for disrupting communications and requires you to confirm your request before proceeding.

Note ▼ This test does not affect the ManageWise software, configuration data, port names, or hub names you have entered. This test does not inject any packets on the network and does not add to the network load.

To run Self-Test 2, click the Self-Test 2 button.

Note ▼ This test might interfere with packet transmission during the time the test is running. Packets received during the test might not be relayed and, therefore, lost. If you are concerned about maintaining network integrity during the test, use Self-Test 1 to test the hub.

You can click the Exit button at any time during the hub hardware reset or self tests to exit the Hub Fault Test dialog box. This action does not halt the test on the hub, however, and you do not see the results of the test when the test is completed.

Monitoring Hub Performance

ManageWise allows you to monitor hub performance to display real-time data as it is received. You can view the current data and also compare it with data received previously.

Note ▼ ManageWise does not store performance data. The data is retained only while the graph is displayed.

Ethernet Hub Port Utilization Graph

The Ethernet Hub Port Utilization Graph displays activity on a single port, activity over all the ports on a selected card, activity on selected ports, or all activity on the hub, always on a per-port basis.

Each port is identified on the graph with a different colored line. Use the legend to determine which line corresponds to which port.

To start the Ethernet Hub Port Utilization Graph, follow these steps:

Procedure ▼
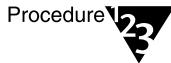
1. **Select a hub, hub card, port, or a combination of these that you want to graph by clicking the appropriate icon.**

   Multiple hubs, cards, or ports can be selected by holding down Ctrl and clicking each of the hubs, cards, or ports you want to select.

2. **Select *Performance > HMI Hub Trends* to display a graph showing activity on the selected object.**

   If a hub port is selected, a graph of activity on the port, or ports, is displayed. This graph displays data as it is collected from the selected hub. This data is not stored in the database, but it provides a dynamic, real-time display of the selected port performance.

Ethernet Hub Port Statistics Table

Data can also be displayed by selecting the Ethernet Hub Port Statistics Table. To display the Ethernet Hub port statistics table, follow these steps:

Note

The active data is not stored by ManageWise. If you want to store data for later review or comparison, use the Print or Export command, described in *ManageWise 2.6 Setup Guide*.

Procedure
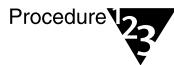
1. **Select the hubs, cards, or ports for which you want statistics.**

2. **Select *Performance > HMI Hub Statistics*.**

A table of data for each of the ports is displayed, as shown in Figure 11-16.

**Figure 11-16
Ethernet Hub
Port Statistics
Table**

Viewing Ethernet Hub Port Statistics

The data available on the Ethernet Hub Port Statistics Table exceeds what can be displayed in the width of the window. Use the scroll bar at the bottom of the window to display all the information described here.

Ethernet Hub Port Statistics Table Fields

The Ethernet Hub Port Statistics Table field information is described in Table 11-2.

Table 11-2
Ethernet Hub Port Statistics Table Fields

Field	Description
Port name	Name assigned to the port by the system administrator.
User name	Login name of the user, if any, currently logged in to the server through the port.
Port ID	Hub number, the card number in the hub, the port number on the card, and the segment value of the port.
Frames/sec	Number of frames per second handled by the port, as reported by the last sampling.
Status	Current port status shown as normal, link down, disabled, or partitioned.
Errors/sec	Number of errors per second at the port, as reported by the most recent sampling.
Bytes/sec	Number of bytes per second handled by the port, as reported by the most recent sampling.
Total frames	Number of frames handled by the port since the hub was most recently brought up.
Total errors	Number of errors on the port since the hub was most recently brought up.
Total bytes	Number of bytes handled by the port since the hub was most recently brought up.
Collisions	Number of collisions on the port since the hub was most recently brought up.
Late events	Number of late collisions on the port since the hub was most recently brought up.
FCS errors	Number of FCS errors on the port since the hub was most recently brought up.
Alignment errors	Number of alignment errors on the port since the hub was most recently brought up.
Frames too long	Number of long frame errors on the port since the hub was most recently brought up.

Table 11-2 *continued*
Ethernet Hub Port Statistics Table Fields

Field	Description
Runts	Number of runts or short frames on the port since the hub was most recently brought up.
Very long events	Number of very long events on the port since the hub was most recently brought up.
Short events	Number of short events on the port since the hub was most recently brought up.
Data rate mismatches	Number of data rate mismatches on the port since the hub was most recently brought up.
Autopartitions	Number of times a device attached to this port was automatically isolated from the network since the hub was most recently brought up. A repeater partitions a station or segment automatically if the station or segment is the source of a large number of consecutive collisions or is the source of abnormally long collisions.
Address changes	Number of times the MAC address for this port changed since the hub was most recently brought up. If this port attaches to another segment, this number is usually large.
Last MAC address	Most recent MAC address observed on the port.

Token Ring Hub Port Statistics Table

The bottom portion of the Token Ring Map window consists of the Token Ring Hub Port Statistics Table. The Token Ring Hub Port Statistics Table displays active data.

Note ▼ The active data is not stored by ManageWise. If you want to store data for later review or comparison, use the Print or Export command, described in *ManageWise 2.6 Setup Guide*.

To display the Token Ring Hub Port Statistics Table, select *Performance > HMI Hub Statistics*. A table of data for each of the ports on the selected hub is displayed, as shown in Figure 11-17.

Viewing Token Ring Hub Port Statistics

The data available on the Token Ring Hub Port Statistics table exceeds
what can be displayed in the width of a window. Use the scroll bar at
the bottom of the window to display all the information described here.

Token Ring Hub Port Statistics Table Fields

The Token Ring Hub Port Statistics Table field information is described
in Table 11-3.

Table 11-3
Token Ring Hub Port Statistics Table Fields

Field	Description
Port name	Name assigned to the port by the system administrator.
User name	Login name of the user, if any, currently logged in to the server through the port.
Port ID	Hub number, card number in the hub, and port number on the card.
Status	Current port status shown as disabled, not inserted, inserted, wrapped, and not wrapped.
Type	Type of token ring port defined as local host, normal, external, ring in, ring out, daisy in, or daisy out.

Table 11-3 *continued*
Token Ring Hub Port Statistics Table Fields

Field	Description
Errors/sec	Errors per second measured at the port.
Total Errors	Number of errors on the port since the hub was most recently brought up.
Line Errors	Number of times a frame or token is copied or repeated by a station since the hub was most recently brought up. More specifically, this error occurs when the following criteria are met: the Error Detected Indicator (E) bit is zero in the incoming frame and one of the following conditions exists: 1. A non-data bit lies between the Start Delimiter and the End Delimiter of the frame or token. 2. An FCS error is in the frame.
Burst Errors	Number of times a station detects the absence of transitions for five half-bit times (burst-five errors) since the hub was most recently brought up.
AC errors	Since the hub was most recently brought up, the number of times a station receives an Active Monitor Present (AMP) or Standby Monitor Present (SMP) frame in which the AC bits are equal to zero. The same station then receives another SMP frame with AC bits equal to zero without first receiving an AMP frame.
Abort Transmissions	Number of times a station transmits an abort delimiter during transmission since the hub was most recently brought up.
Internal errors	Number of times a station recognizes an internal error since the hub was most recently brought up.
Duplicate Addresses	Number of times a duplicated address was detected on the ring since the hub was most recently brought up.
Receive Congestions	The number of times a station recognizes a frame addressed to it, but has no available buffer space to copy it, since the hub was most recently brought up.
Bcn. Set Recovery	Number of Claim Token MAC frames received or transmitted after the repeater has received a Ring Purge MAC frame since the hub was most recently brought up. This counter signifies the number of times the ring has been purged and is set to recover to a normal operating state.
Bcn. Signal Loss	Number of times the repeater has detected a signal loss from the ring since the hub was most recently brought up. This condition is usually the result of a broken ring, faulty wiring at the concentrator end, transmitter malfunction, or receiver malfunction.

Table 11-3 *continued*
Token Ring Hub Port Statistics Table Fields

Field	Description
Bcn. Streaming	A combination of counters: bit streaming and frame streaming. The bit streaming counter removes (destroys) tokens and frames by writing over (repeat and transmit both occurring) or replacing (uncontrolled transmit) ring data. This process initiates monitor contention. Frame streaming is continuous transmission of tokens, abort sequences, or frames.
Functional Address	Group address of the port that provides a well-known address for network functions such as active monitor, ring error monitor, and so on.
Address Changes	Number of times the last address changed since the hub was most recently brought up.
Last MAC Address	The physical (MAC) address of the most recent device attached to the port.
Neighbor Changes	Number of times the downstream neighbor changed since the hub was most recently brought up.
Neighbor Address	Physical (MAC) address of the downstream station.

Configuring Hubs and Ports

In addition to the system configuration modifications described in *ManageWise 2.6 Setup Guide*, you can use the Configure menu to change names assigned to hubs and ports, to enable and disable ports, and to configure new port segments.

Changing Hub and Port Names

To change or enter a name, select the hub or port by clicking the appropriate hub or port icon. The selected hub name or port number is highlighted, indicating it has been selected.

Note ▼ Select a hub on a Custom hub backpanel by holding down Shift and clicking a hub card.

Next, select *Configure > HMI Hub > Name*. The Change Hub Name or Change Port Name dialog box appears. Figure 11-18 shows the Change Hub Name dialog box. Enter the new name for the selected object, then click the Change button. A Confirmation dialog box appears, which prompts you to confirm the new name for the selected device. Click OK to make the change.

**Figure 11-18
Change Hub
Name Dialog Box**
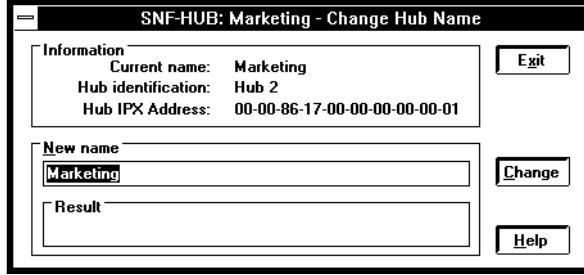
Enabling or Disabling a Port

The Configure menu allows a selected port to be enabled or disabled. The condition for which the port is currently configured is disabled. The solid type indicates the port status after the command is executed.

To change the status of a port, select *Configure > HMI Hub > Port Enable* to enable the port or *Configure > HMI Hub > Port Disable* to disable the port.

Configuring a New Port Segment

The Configure menu allows a selected port or ports to be moved to another segment. To change the segment that a port is currently attached to, select the port whose segment you want to change, and then select *Configure > HMI Hub > Port Segment*. The Configure Port Segment dialog box, Figure 11-19, is displayed.

**Figure 11-19
Configure Port
Segment
Dialog Box**
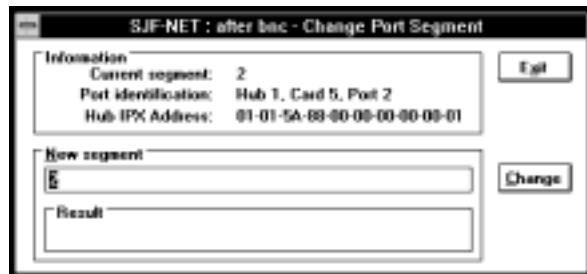
You can change the port segment by typing the number of a different segment in the New segment text box.

Minimizing Windows

Figure 11-20 shows samples of some icon types you can produce when you minimize hub-related windows in ManageWise.

Figure 11-20
Icons of Minimized Hub-Related Windows
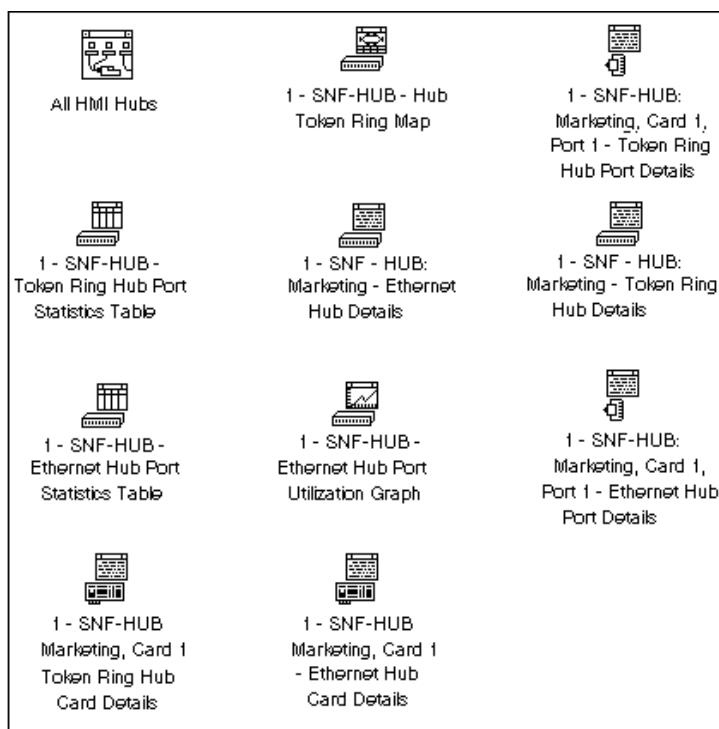
Whenever you minimize a window to an icon, the function is still running but the window no longer takes space on your desktop. A typical use is to minimize a graph to its icon, allowing it to continue to gather data while you examine other aspects of your network.

Tips and Techniques

This section provides tips and techniques for using the hub-related services of ManageWise.

Enabling and Disabling Ports

You might want to disable ports for any of several reasons:

◆ For operational reasons. Disabling a malfunctioning station removes it from the network so it does not interfere with the operation of other stations.

◆ For administrative or security reasons. Disabling a port that connects to another hub or to a bridge isolates the hub from other segments.

◆ To improve network performance. Disabling a port when the network is heavily loaded and connectivity to other segments is not needed (for example, during disk backup at night) can improve performance.

When you enable or disable a port, the port state value is usually saved when power fails. However, some hub cards temporarily allow disabled ports to become enabled when the server is restarted. If this is a serious concern for you, check with your hub card vendor.

Naming Ports

Naming ports can simplify your network administration tasks and can help you identify the machine that is attached to the port. For more information, refer to Table 11-3 on page 300.

Typically, the name of the person who uses the computer connected to the port or the number of the office wired to the port is used for the port name.

ManageWise automatically sets the port name based on the login name (except SUPERVISOR and GUEST) if the port name contains "N/A." This occurs only if the client node connected to the port logs in to the server containing the hub. *The login name never overrides a manual setting.*

Understanding the Typical Operation of Your Network

Understanding the typical operation of your network helps you recognize the symptoms your network shows when it is operating less than optimally. The Ethernet and Token Ring Hub Details windows (Figure 11-6 and Figure 11-9), Hub Card Details windows (Figure 11-7 and Figure 11-10), and Hub Port Details windows (Figure 11-8, Figure 11-11, and Figure 11-12) provide overviews of the current state of the network that is both condensed and easy to examine.

You should become familiar with these windows to understand what they look like when your network is operating normally. If you know the normal behavior of your network, you can quickly recognize when there is a problem and correct it.

Isolating and Disabling Sources of Network Errors

Errors are indicated by a change in color of the port icon in either the Hub Port Map or Hub Backpanel window.

The Hub Port Details windows provide more detailed information about the type of error that has occurred. If you observe continuous errors, the port should be disabled until the problem is corrected. Disabling the port removes the faulty equipment from the network. Most errors are caused by a hardware problem, such as bad cabling or a faulty network card connected to the port.

Hub Errors

This section tells you what to do when the transmit collisions and very long event hub errors occur.

Transmit Collisions

Transmission errors are a normal part of Ethernet behavior and are not important unless the collision rate is more than 10 collisions per second. A high collision rate often indicates that the network is overloaded, but faulty equipment can also cause a high collision rate.

If more than 30 consecutive collisions are observed on a port, the port is automatically isolated (*autopartitioned*), thus removing the connected equipment from the network while the condition persists.

When the hub has a high collision rate, examine the Hub Port Statistics Table to determine whether a single port is causing the majority of the transmit collisions or the port link state is partitioned. If either of these conditions is occurring, disable the port. Then refer to the "Collisions" and "Partitions" tips.

Very Long Events

Very long events cause the repeater to enter MAU Jabber Lockout Protection (MJLP). They do not occur on a healthy network. Very long events are usually caused by a bad controller card or bad wiring.

Use the Hub Port Statistics Table to determine which port is the cause. Disable the port. Then refer to the "Very Long Events" tip in "Port Errors."

Port Errors

This section tells you what to do when various port errors occur.

Frame Check Sequence Errors

FCS errors, alignment errors, and short events are usually caused by electrical noise picked up by the wiring.

Test the wiring. If it runs near power cables, electrical equipment, and so forth, it might need to be replaced or rerouted.

Alignment Errors

Refer to "Frame Check Sequence Errors."

Short Events

Refer to "Frame Check Sequence Errors."

Frames Too Long

Frames too long are usually created by a bad network controller connected to the port. Disable the port, replace the controller, and enable the port.

Software that violates the IEEE 802.3 specification can also be a source of frames that are too long.

Runts

Runts should not occur unless the port connects the repeater to a coaxial Ethernet cable or another 10BASE-T repeater. Repeaters generate runts by transmitting jam sequences on all ports of the repeater to signify that a collision has occurred. A repeater does not count the runts it generates, but it does count runts coming from another connected repeater.

If a port connected to a workstation is seeing runts, the port should be disabled. The network card in the workstation should be checked and replaced, if necessary.

Collisions

Collisions are a normal event on Ethernet networks. They are a problem only if they become excessive. The repeater hardware automatically isolates (partitions) ports that cause 30 consecutive collisions. If the collision rate of a port exceeds five percent of the port packet rate, it might indicate a problem.

If the collision rate of a port exceeds five percent, the port should be disabled. The network card attached to the port should be checked and replaced, if necessary.

Late Events (Late Collisions)

Late events (late collisions) should never occur. They are collisions that have violated the Ethernet specification. They can be caused by a faulty network card or an improperly configured network (more than three repeaters/hubs in a series between any two nodes on the network).

If your network is configured properly, disable the port and replace the network card for the connected station.

Data Rate Mismatches

Data rate mismatches should never occur. They are caused by an out-of-specification oscillator on the network card attached to the port.

If all (or a number) of ports report data rate mismatches, the hub card contains a faulty oscillator. Replace the hub card.

If only one port is reporting this condition, disable the port and replace the network card in the connected station.

Partitions

When a hub partitions a station that is attached to a port, it isolates the station from the rest of the network. Partitions indicate that the connected station is creating too many collisions or excessively long collisions. This is usually caused by a faulty network card.

Disable the port and replace the network card in the connected station.

Very Long Events

Very long events are usually caused by a bad network controller connected to the port or bad wiring.

Disable the port, replace the controller card, and enable the port. If that does not fix the problem, test the wiring.

Interpreting the Source Address Change Count

The source address change count increases every time a new node address is observed transmitting on the port. If no packets have ever been sent, the change count is zero. Usually, the change count is one, indicating that only one workstation is using the port.

This field lets you determine when users have been moving equipment on their own, which is a common source of problems.

If the count changes frequently, the port is most likely connected to another hub, a coaxial Ethernet cable, or a MAC bridge. If the change count is a small number and does not change frequently, the equipment connected to the port has probably been changed.

Determining Wiring Integrity

The integrity of a twisted-pair connection between the hub and the attached equipment is indicated by the port link state. If the Hub Port Details window for a selected port shows the Link Up state, the 10BASE-T wiring is connected and the attached device (computer, node, or other equipment) is turned on. If the window shows the Link Down state, the port is not connected, the equipment at the other end is not turned on, or the wiring is bad.

If the Hub Port Details window shows the Link Down state for a 10BASE-T port that is connected to turned-on equipment, there is a problem with the wiring or the attached equipment.

Determining Current Network Utilization

The Ethernet and Token Ring Hub Port Statistics windows, Figure 11-16 and Figure 11-17, help to indicate the heaviest users of the network. If a sustained high utilization rate is frequently observed, it might indicate that the network should be segmented by adding a router or a bridge. For more information, continue to the next tip.

Reconfiguring a Heavily Utilized Network

If your network has a sustained high utilization rate (over 30 percent), you might consider reconfiguring the network by using a router to segment it. Your NetWare server can act as a router by simply adding one or more additional hubs or LAN boards to the server. The NetWare MultiProtocol Router™ software can also be used to route network traffic between hubs. The routing function of the server limits the network traffic to only those hubs that need to see it, thus reducing the utilization on all the hubs.

For optimum performance, you should organize your network so that client workstations attach to the same hub as the server they usually use.

Refer to the "Routing" section of *NetWare Version 3.11 Concepts* and to *NetWare Version 3.11 TCP/IP Transport Supervisor's Guide* for more information about using your server as a router.

Hub Security Issues

Some network installations use the port control feature as a means of instituting security. Ports that are not used are typically disabled.

However, some hub cards allow disabled ports to become enabled temporarily when the server is turned on. If you are concerned about security, check with your hardware vendor to determine whether your hub hardware ensures that disabled ports never become temporarily enabled when they are turned on.

Minimizing Resource Utilization

ManageWise hub-related software consumes resources in two ways:

◆ Processing time required to update the windows

◆ SNMP network requests to retrieve data

The processing time depends on the number of ports in the hub and the sampling interval used to update statistics. Increasing the sampling interval to a large time (for example, 2 minutes) reduces the CPU load and network traffic.

Hub Alarms

This section explains hub-related error messages generated by ManageWise and steps you can take to enhance system performance.

Error Messages

Error and information messages can be displayed in various contexts to indicate a problem or a failure to complete an operation. Some of these might appear when a window is opened, some appear inside dialog boxes, and others appear when appropriate. Here is a list of these messages.

SNMP Data Server Is Not Active

This message is displayed whenever you attempt to open a window that requires data communication with one or more hubs and the SNMP Data Server is not running properly. Without the SNMP Data Server, ManageWise cannot get the requested data.

Action: Restart the SNMP Data Server by double-clicking the ManageWise icon on your ManageWise Console.

If the SNMP Data Server goes down while a window is active, the window mode changes to "Terminated." Restarting the SNMP Data Server does not automatically make the window active again. You must close and reopen the window to make the window active.

Data Communication Error Messages

The following messages indicate a data communications failure. These messages appear in several forms and in several contexts:

◆ Error accessing hub

◆ Insufficient resources to connect

◆ Unable to complete Hub Reset operation

◆ Unable to complete Hub Self-Test 1 operation

◆ Unable to complete Hub Self-Test 2 operation

◆ Unable to change port status

◆ Unable to change hub name

◆ Unable to change port name

◆ Cannot access hub

ManageWise data communications failure could be due to any of the following:

◆ Specified hub does not exist or is not active.

◆ Specified hub is not linked over the network to the console.

◆ SNMP Agent is not loaded or is not properly configured, or NetWare Hub Services NLM files are not running on the hub.

◆ Hub is not accessible due to improper settings of the SNMP Agent.

◆ Network error rate or traffic volume is high and the data request or the response did not go through within the allocated time.

◆ Data responses are lost because the ManageWise Console has too many windows open or is using too many resources so that data responses are not buffered.

◆ Windows cannot start data requests because the ManageWise Console does not have sufficient resources.

Action: Perform the following checks and procedures:

◆ Check that both server and ManageWise Console hardware are functioning correctly.

◆ Check wiring.

◆ Close as many windows as possible on the ManageWise Console to reduce network traffic and messages between windows.

◆ Verify that the SNMP Agent parameters match the values set on the ManageWise Console.

◆ Update the SNMP Agent.

◆ Increase memory or drive capacity on the ManageWise Console.

Performance

When you open many windows at the same time, are processing data requests, and are processing window updates, Windows slows down considerably. The following are symptoms that your ManageWise Console is overloaded:

◆ Windows takes a long time to respond to a mouse click or key stroke.

◆ Some messages are lost because the Windows message queue is full. When this happens, ManageWise windows stay in the "Connecting" or "Obtaining Data" mode forever.

◆ Expected actions might not happen because Windows has stopped sending timers properly.

◆ Data requests might fail, causing ManageWise hub-related windows to change to "Inactive," "Connection Failed," or other modes.

◆ Windows is consuming so many resources, such as memory, that it loses data.

Action: Perform the following corrective actions to reduce the load on Windows:

◆ Reduce the number of windows. This reduces the network data request traffic and frees ManageWise Console resources, thereby improving ManageWise response time.

◆ Modify the HSM.INI file to slow the data update rates for various windows. A rule of thumb is to make update intervals long enough to allow about five seconds per hub card.

For example, if you want to display the following:

  ◆ Two Backpanel windows

  ◆ One Port Map window

  ◆ Hub Port Statistics Table window

  ◆ Each window displaying data from three cards

You can calculate a suggested update interval for those windows using the following formula:

number of cards x 5 = number of seconds for each window

For example, with 12 cards, allow 60 seconds. The suggested 5 seconds per hub card is for cards with 12 to 15 ports. If your hub card has more ports, 24 for example, increase the suggested interval accordingly.

Changes you make to an update interval in the HSM.INI file do not affect any window that is already opened.

chapter **12** *Managing SNMP Devices*

ManageWise® software enables you to manage any SNMP-manageable device on your network. In particular, ManageWise does the following:

◆ Receives alarms, often referred to as *SNMP traps*, from these devices. For further information about receiving alarms, refer to Chapter 6, "Understanding Alarms."

◆ Uses the Novell® Management Information Base (MIB) Browser to display and set values on these devices.

Before ManageWise can interpret SNMP alarms from devices, and before you can use the MIB Browser to manage those devices, you need to perform certain tasks. This chapter explains those tasks and discusses how you can use the MIB Browser to manage SNMP devices.

Getting Started

You need to perform the tasks in the following sections to prepare ManageWise to interpret SNMP alarms from devices and before using the MIB Browser:

◆ Acquiring MIBs

◆ Adding Trap Annotations, if desired

◆ Compiling MIBs, if you need to add new MIBs or remove MIBs that you no longer need

This section explains how to perform these tasks.

Acquiring MIBs

To manage a device, you must first obtain a copy of the MIB or MIBs that the device supports. A MIB is simply an ASCII text file, written in a precise format, that describes the management information available on a particular class of devices. If, for example, you have an XYZ router from company X and you want to use ManageWise to manage the router, company X must provide you with the XYZ router MIB.

Important ▼ If you want to compile any new MIBS, you must store them in the \MW\NMS\SNMPMIBS\CURRENT directory. Otherwise, you can store them in the \MW\NMS\SNMPMIBS\ALLMIBS directory.

ManageWise is shipped with many standard and vendor-proprietary MIBs that reside in the \MW\NMS\SNMPMIBS\ALLMIBS directory. However, only the most general of these MIBs are actually compiled into the ManageWise product.

Adding Trap Annotations

Some SNMP MIBs define the traps that a device can send to the ManageWise Console when an unusual event occurs on the network. When you compile a MIB containing traps (refer to "Compiling MIBs" on page 325), information about those traps is added to the ManageWise alarm database. When ManageWise receives such a trap, the information in the alarm database is retrieved and used by ManageWise to generate the alarm summary string and to determine the alarm type, alarm severity, state of the affected device, and so forth.

You can improve the presentation of the alarm information in ManageWise by adding annotations to the trap definitions in the MIB file. These annotations are added as comments to the trap definitions so that the MIB still compiles with third-party MIB compilers.

All Novell MIBs are annotated. If you choose not to annotate the traps in other MIBs, ManageWise still displays the alarms; however, they are less readable.

SNMP MIBs use the TRAP-TYPE macro to define traps. Figure 12-1 shows an example of a trap definition.

```
dupIpxNetAddr          TRAP-TYPE
   ENTERPRISE          netware-GA-alert-mib
   VARIABLES           {osName, osLoc, tiTrapTime, tiEventValue,
                       tiEventSeverity, tiServer}
   DESCRIPTION         "Two servers use the same IPX internet address."
   : :=8
```

dupIpxNetAddr is the name of the trap. (It means duplicate IPX™ network address.)

The ENTERPRISE clause contains the OBJECT IDENTIFIER of a node in the vendor's tree, which, together with the trap number (the **8** following the ": :=" in Figure 12-1), uniquely identify the trap.

The VARIABLES clause defines an ordered sequence of MIB objects that are passed as parameters of the trap to provide additional information about the event. For example, *osName* is a text string specifying the name of the server sending the trap; *osLoc* is a text string specifying the location of the server; *tiTrapTime* is an integer specifying the time the event occurred.

The DESCRIPTION clause provides a textual description of the semantics of the trap.

The ": := 8" clause identifies the trap.

Table 12-1 lists and explains the keywords you can use to annotate traps.

Table 12-1
Keywords for Annotating Traps

Keyword	Explanation
--#TYPE	Short name for the alarm. The name can be a maximum of 40 characters. In the absence of this annotation, the SNMP trap name is used.
--#SUMMARY	Description of the alarm with placeholders and formatting information for the actual parameters passed with the alarm. For further information about formatting the summary, refer to the section "Formatting the SUMMARY String" on page 323. Without this annotation, the alarm summary string is a list of each SNMP parameter name followed by its value.
--#ARGUMENTS	List of parameters to substitute in the SUMMARY string. Parameters are substituted in the order in which they appear in the list. Each element of the list is the (zero-based) index of the parameter in the $VARIABLES$ clause.
--#SEVERITY	Default severity assigned to the trap. This can be one of the following: ◆ INFORMATIONAL ◆ MINOR ◆ MAJOR ◆ CRITICAL ◆ UNKNOWN Alarms with a default severity set to CRITICAL are displayed in the ticker tape. Without this annotation, the severity is displayed with the value UNKNOWN.
--#TIMEINDEX	Index of the variable in the $VARIABLES$ clause. This index contains the time when the alarm was generated. The time is expected to be an integer representing the number of seconds since 1970 ("UNIX time"). If such a variable does not exist in the $VARIABLES$ clause, use an index greater than the total number of variables in the $VARIABLES$ clause.
--#HELP	Name of the help file that contains information about the alarm. This is a Windows 3.1 online help file with the extension .HLP. This file must be placed in the ManageWise help path directory. Without this annotation, no alarm-specific help is available.

Table 12-1 *continued*
Keywords for Annotating Traps

Keyword	Explanation
--#HELPTAG	Integer context tag in the help file for this alarm.
	Without this annotation, no alarm-specific help is available.
--#STATE	Default state of the object when the alarm was generated. This can be one of the following:
	◆ OPERATIONAL
	◆ NONOPERATIONAL
	◆ DEGRADED
	◆ UNKNOWN
	Without this annotation, the state is displayed with the value UNKNOWN.

Figure 12-2 shows the `dupIpxNetAddr` trap with annotations added to it.

Figure 12-2
Annotated Trap
Definition

```
dupIpxNetAddr          TRAP-TYPE
  ENTERPRISE           netware-GA-alert-mib
  VARIABLES            {osName, osLoc, tiTrapTime, tiEventValue,
                       tiEventSeverity, tiServer}
  DESCRIPTION          "Two servers use the same IPX internet address."


  --NMS trap annotation

  --#TYPE              "Duplicate IPX address"
  --#SUMMARY           "%s at %s and %s are using the same IPX address"
  --#ARGUMENTS         {0, 1, 5}
  --#SEVERITY          CRITICAL
  --#TIMEINDEX         2
  --#HELP              "MYHELP.HLP"
  --#HELPTAG           60004
  --#STATE             DEGRADED
  : :=8
```

Note the following rules about adding annotations:

◆ Each annotation must be embedded in a comment. Everything from the double hyphen to the end of the line is treated as a comment (refer to Figure 12-2).

◆ Each annotation must be on a separate line.

◆ Annotations must appear in the order in which they are discussed in Table 12-1.

◆ All annotations must be inserted after the DESCRIPTION clause and before the ": := " clause.

◆ STATE and SEVERITY values are written to the alarm database the first time the MIB is compiled, so any changes you might make by selecting *Fault > Alarm Disposition* do not get overwritten. If you do want to overwrite the existing values, you must run the Compiler (MIBC.EXE contained in \MW\NMS\BIN) from the Program Manager *File > Run* menu with the following command-line argument:

MIBC.EXE −F *filename* **[-S]**

The variable *filename* is the name of the MIB file for which you want the overwrite to occur. The optional -S switch (silent mode) causes the Compiler to run in the background. We recommend that third-party developers use silent mode.

Displaying Annotated Traps in ManageWise

Assume that the dupIpxNetAddr trap, shown in Figure 12-1, was received by ManageWise with the following variables:

◆ *osName* = SJM-JACK

◆ *osLoc* = JACK's CORNER

◆ *tiTrapTime* = ~700000000

◆ *tiServer* = SJM-TIM

To display a trap, use the Alarm Monitor or Alarm Report table. The tables would display the trap as shown in Figure 12-3.

```
Receive Time:        08/21/92 09:15:45
Alarm Type:          Duplicate IPX address
Summary:             SJM-JACK at JACK's CORNER and SJM-TIM are
                     using the same IPX address
Severity:            Critical
State:               Degraded
```

When you select the alarm on the Alarm Report table and click the
NetWare® Expert™ button, ManageWise displays help information for
this alarm.

Formatting the SUMMARY String

The SUMMARY keyword in the trap annotation lets you provide the
actual wording of the alarm summary. This wording is used by
ManageWise when the alarm occurs. Placeholders within the string are
replaced by actual parameters of the trap before the string is displayed
by ManageWise. Each placeholder format string begins with a "%" sign
and tells ManageWise how to format the parameter that will be
substituted for the placeholder in the final string. Table 12-2 lists all the
available format strings for each parameter type and indicates the
printed form for each value.

The placeholder format strings are substituted, in order, by the
parameters specified in the ARGUMENTS keyword. The
ARGUMENTS keyword lists the (zero-based) index of each trap
parameter as specified in the VARIABLES clause. The indexes are listed
in the order in which you want them to be substituted in the
SUMMARY string.

ManageWise can display a maximum of 140 characters in the
SUMMARY string. You must use the characters to display the most
relevant information about the alarm. If you have a long SUMMARY
string and want to keep the line length of the MIB file reasonable, you
can insert multiple, consecutive, SUMMARY annotations and the
strings will be concatenated. For example, the two annotations below
yield the same string:

```
--#SUMMARY     "%s at %s and %s are using the same "
--#SUMMARY     "IPX address"


--#SUMMARY     "%s at %s "
--#SUMMARY     "and %s are "
--#SUMMARY     "using the same IPX address"
```

Table 12-2
Format Strings and Parameter Types

Parameter Type	Format String	Printed Form
BOOLEAN	%s	"True" or "False."
	%d	1 or 0.
INTEGER	%x	HEX.
	%d	Decimal.
	%t	Prints the integer or a date and time (GMT). The integer represents seconds since 1970.
OCTET STRING	%s	Text string with all control characters stripped out.
	%m	Prints the first 6 bytes of data as a hyphen-separated MAC address. For example, 00–00–07–00–07.
	%x	Prints the octet string in hexadecimal. For example, 0000070007.
NULL	%d	Prints the number '0.'
	%s	Prints the string "NULL."
OBJECT IDENTIFIER	%s	Dot-separated decimal values. For example, 1.3.6.5.4.
IP ADDRESS	%s	Dot-separated IP address. For example, 13.56.56.56.
	%x	Long hexadecimal value.
BIT STRING	%s	Each byte printed as decimal.

Resetting Traps

Traps are defined by SNMP MIBs; therefore, resetting traps resets SNMP MIBs. The process of resetting traps removes traps that you no longer need.

To reset compiled SNMP MIBs, follow these steps:

Procedure 23

1. **Remove the unwanted MIB from the \MW\NMS\SNMPMIBS\CURRENT directory.**

2. **Start the Database Administration Tool as described in "Starting the Database Administration Tool" on page 92.**

3. **Select *Reset Traps*.**

   All compiled MIBs are removed from the ManageWise database and the existing alarm file is overwritten by the empty TRAP.BTV alarm file.

4. **Exit the Database Administration Tool.**

5. **Open ManageWise and run the MIB compiler by selecting *Tools > SNMP MIB Compiler*.**

   All alarm definitions from the MIBs in the ...\CURRENT directory are placed into the TRAP.BTV file.

Compiling MIBs

Having obtained additional necessary MIBs, you must copy them into the \MW\NMS\SNMPMIBS\CURRENT directory. Remove any MIBs in the ...\CURRENT directory that you do not need. (Make sure you have a copy in the \MW\NMS\SNMPMIBS\ALLMIBS directory.) When the ...\CURRENT directory contains all the MIBs you want to integrate into ManageWise, run the SNMP MIB compiler. Figure 12-4 demonstrates how the SNMP MIB compiler incorporates information from the MIBs into the appropriate ManageWise files.

Figure 12-4
SNMP MIB Compiler
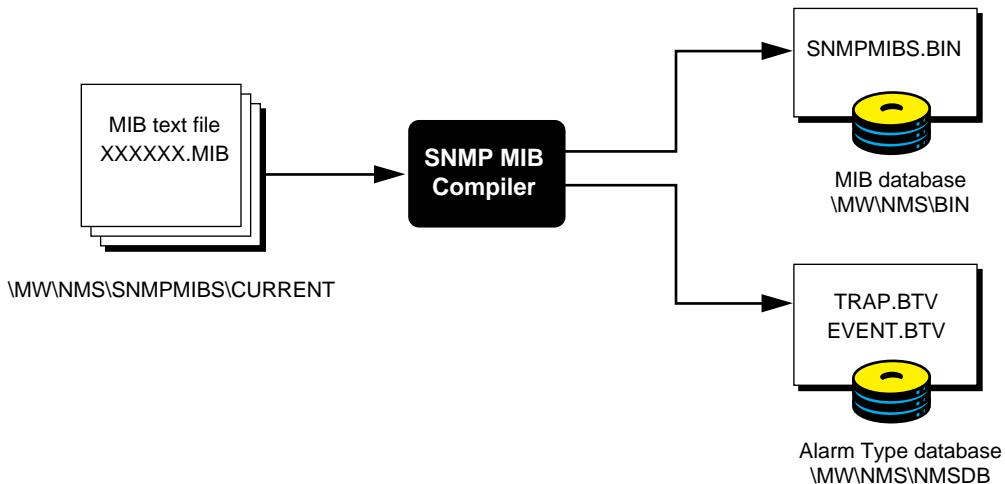
To run the SNMP MIB Compiler, select *Tools > SNMP MIB Compiler*. The SNMP MIB Compiler compiles all the MIB text files in the \MW\NMS\SNMPMIBS\CURRENT directory into a single binary file, \MW\NMS\BIN\SNMPMIBS.BIN, for use by the SNMP MIB Browser and the SNMP protocol decoder. The MIB Compiler also adds or updates any trap definitions to the Alarm Type database files, \MW\NMS\NMSDB\TRAPS.BTV and EVENT.BTV, for use by the ManageWise alarm subsystem.

We recommend that you keep a complete set of all the MIBs you acquire in the \MW\NMS\SNMPMIBS\ALLMIBS directory and then copy the ones you want to be part of ManageWise into the \MW\NMS\SNMPMIBS\CURRENT directory.

To delete a particular MIB from ManageWise, delete the appropriate MIB text file from the ...\CURRENT directory and rerun the SNMP MIB Compiler. If the MIB you delete contains traps and you also want to remove the alarm definitions from ManageWise, use the Database Administration Tool to remove the alarm definitions before you rerun the SNMP MIB Compiler. For information about the Database Administration Tool, refer to "Maintaining the ManageWise Database" on page 92.

Using the MIB Browser to Manage SNMP Devices

The SNMP MIB Browser lets you issue SNMP requests to any SNMP Agent on the network and display the results of SNMP requests in tables or graphs. As a result, you can manage many of your network devices prior to integrating additional applications. This tool requires some knowledge of SNMP.

Using the MIB Browser, you can retrieve specific device information (GET) and specify where to get the information. You can also change information at the target device (SET) if you have the appropriate access to that device.

You use a *profile* to specify the information you want and how often you want to poll for it. A *profile* is an ASCII file (much like the Windows initialization file) that specifies the following information:

- ◆ Profile description

- ◆ Mode of operation (once or polled)

- ◆ Polling interval

- ◆ Method of display (table or graph)

- ◆ One or more attributes to retrieve from the target device

You can edit, create, or delete profiles.

Retrieving an IPX or IP Device

The SNMP MIB Browser sends a GET request to the target device and retrieves the values of the attributes specified in the profile. The SNMP MIB Browser looks for the information using the IPX or IP address of the device. You can access an IPX or IP device in two ways:

- ◆ By selecting the device using a map

- ◆ By specifying the IPX or IP address of the device

Accessing a Device Using a Map

If you access the SNMP MIB Browser after selecting a device on a map, the SNMP MIB Browser starts and displays the IPX or IP address for that device in the SNMP MIB Browser dialog box, as shown in Step 2.

To access the device, follow these steps:

Procedure

1. **Select the device icon on any map.**

2. **Select *Tools > SNMP MIB Browser*.**

   The SNMP MIB Browser dialog box is displayed:
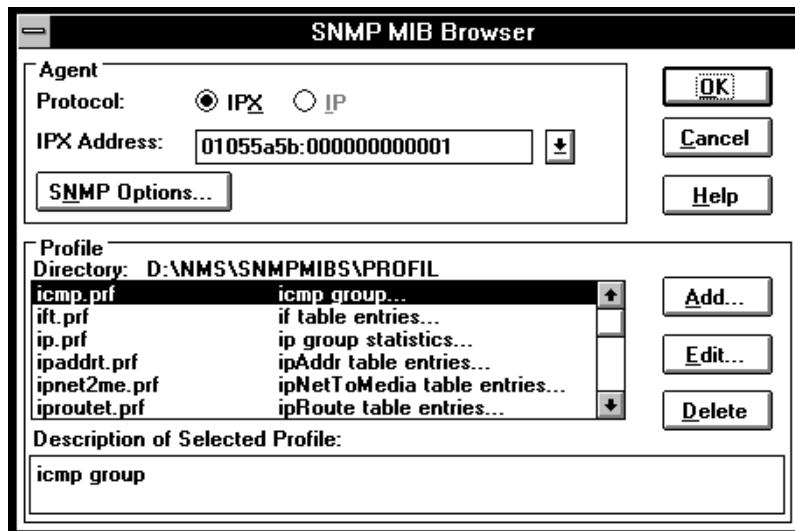
This dialog box contains the following fields and buttons:

◆ **Protocol**—Specified by clicking the appropriate option button. The target device address can be either IPX or IP.

◆ **Address**—Actual IPX or IP address of the target device.

◆ **SNMP Options**—Displays a window you can use to change the community string used in the SNMP request. The default community string is set in Global Preferences. Refer to "Setting the Community Strings" on page 329 for more information.

- ◆ **Profile**—Lists the available profiles.

- ◆ **OK**—Processes an SNMP request.

- ◆ **Cancel**—Cancels a session.

- ◆ **Help**—Displays the help window.

- ◆ **Add**—Displays a create profile dialog box.

- ◆ **Edit**—Edits an existing profile or attribute.

- ◆ **Delete**—Deletes a profile.

Specifying the IPX or IP Address

If you have not selected the target device from a map, or if the device does not have an icon on the map, you can still access the device with the SNMP MIB Browser if you have the IPX or IP address of the device.

To access a device that does not have an icon on the map, follow these steps:

Procedure
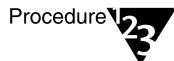
1. **Select *Tools > SNMP MIB Browser*.**

   The SNMP MIB Browser dialog box is displayed.

2. **Click the IPX or IP option button.**

3. **Type the address in the address box.**

From this point, you can use the SNMP MIB Browser to display SNMP data, as described in "Displaying SNMP Data" on page 332.

Setting the Community Strings

By default, ManageWise applications use the community string "public" for SNMP GET and SET operations. The SNMP Options dialog box enables you to configure different community strings for each device on the network. After this information is entered for a device, it is used instead of the defaults whenever a ManageWise application uses SNMP to communicate with that device.

The SET community string is used in SNMP SET operations and the GET community string is used in SNMP GET operations. If the community string used by ManageWise does not match the one expected by the SNMP Agent in the managed device, the operation fails. SNMP community strings are transmitted in clear text in each SNMP request and, therefore, provide only a rudimentary form of security.

To provide greater security, Novell has implemented SNMP over the connection-oriented NetWare Core Protocol™ (NCP™) protocol, which is used for all NetWare client-server interactions. When the server receives an SNMP packet over NCP and the NCP connection has either SUPERVISOR or OPERATOR privileges, the SNMP Agent bypasses the normal community string checks. If the connection does not have sufficient privileges, the community string is checked as usual.

To prevent unauthorized users from performing SNMP SET operations to a NetWare server, disable the SET community at the server so only authorized NetWare users using SNMP over NCP can perform SETs.

Note   When SNMP is installed initially on the NetWare server, the SET community is disabled and the GET community is set to "public"; however, some products, such as NetWare LANalyzer® Agent™ software, modify the SNMP community settings as part of their installation process.

You can also (independently) disable the GET community and thus only allow GET operations by authorized NetWare users using SNMP over NCP. Do this only when absolutely necessary because there is a performance penalty at the ManageWise Console caused by the synchronous nature of the NCP APIs. This is not a problem when using SNMP over NCP for SETs, because SET operations are infrequent compared to GET operations.

The Login for Set and Login for Get check boxes in the SNMP Options Setup dialog box enable you to specify whether to use SNMP over NCP for SETs and GETs. If you check the Login for Set box, you are asked to log in to the server (or tree) when you try to perform a SET operation to that server. If you already have a connection to that server, it is used and you need not log in again.

To set the community strings, follow these steps:

1. Select a device from any map or table.

2. Select *Configure > SNMP Options*.

The SNMP Options Setup dialog box, Figure 12-5, is displayed.

Figure 12-5
SNMP Options
Setup Dialog Box
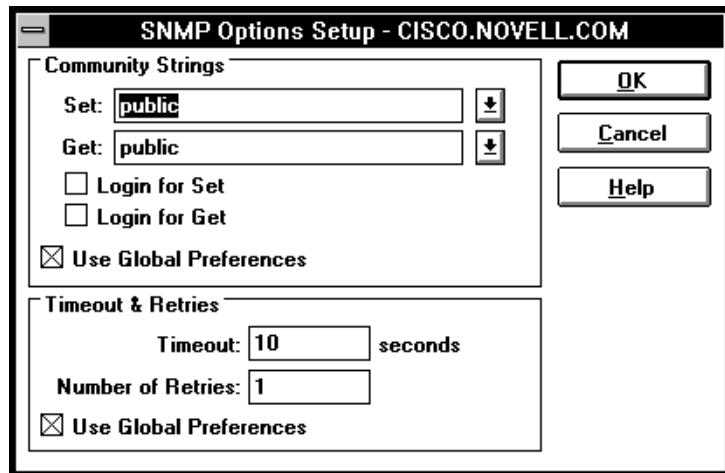
3. Type the community string for ManageWise to use when communicating with that device.

The community string is stored in the database for ManageWise to use. If the device is not in the database, ManageWise creates an SNMP.INI file and stores the strings in it.

4. Select the Login for Set or Login for Get check boxes, as desired.

5. Click OK.

Note ▼ For devices not in the ManageWise database, community string changes do not take effect if you are using IP. Therefore, if you use IP, you must also change the IP community string. To do so, select *File > Open > File Server*, enter the IP address of the server, and follow the procedure from Step 3 on page 331.

Displaying SNMP Data

To use the MIB Browser to display SNMP data, follow these steps:

Procedure

1. **Select *Tools > SNMP MIB Browser*.**

   The SNMP MIB Browser dialog box, as shown in Step 2, under the section "Accessing a Device Using a Map" on page 328, is displayed.

2. **Select an existing profile in the Profile selection box.**

   If there is no existing profile that displays the information you want, you can edit or create a profile, as described in the following section, "Editing or Creating a Profile."

3. **Click OK.**

   The system displays the SNMP MIB Browser table with the values of the selected attributes. If you selected the system profile, for example, the attribute information is displayed as shown below:

Refer to the online help for a description of how to use the action bar buttons displayed at the top of the SNMP MIB Browser table.

Editing or Creating a Profile

You can edit a profile to get different attributes. To use the MIB Browser to edit or create a profile, follow these steps:

Procedure 22

1. Select *Tools > SNMP MIB Browser*.

The SNMP MIB Browser dialog box, as shown in Step 2 under the section "Accessing a Device Using a Map" on page 328, is displayed. A list of existing profiles, along with a description of the selected profile, is displayed in the Profile selection box.

2. Select an existing profile and click Edit to edit a profile or click Add to create a new profile.

The SNMP Profile Editor dialog box is displayed:
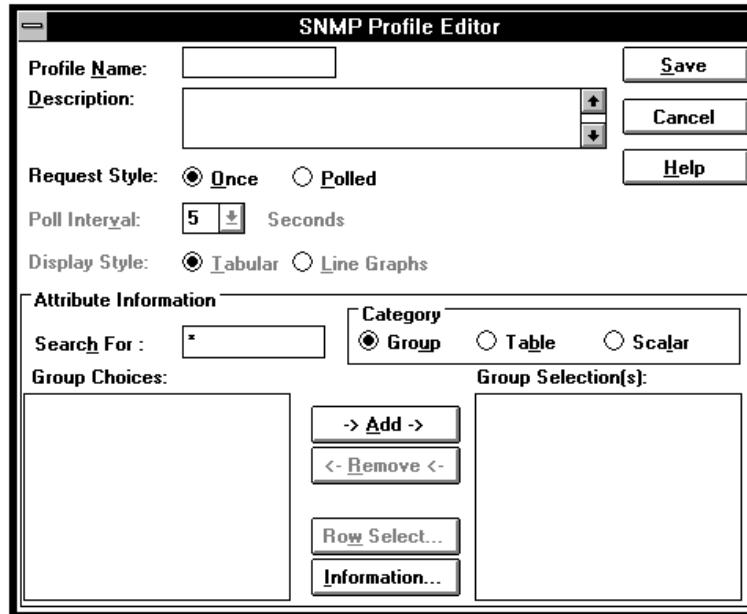
Refer to the following section, "SNMP Profile Editor Fields," for a description of the fields in this dialog box.

3. Save the profile you edited.

The SNMP MIB Browser dialog box is displayed again.

SNMP Profile Editor Fields

The SNMP Profile Editor dialog box contains the following fields and buttons:

◆ **Profile Name**—Describes the selected profile name. If you enter a new filename, a new file is created when you click Save.

◆ **Description**—Provides a textual description about what the profile does. This allows you to enter free-format text.

◆ **Request Style options**—Can be one of the following:

  ◆ **Once**—Requests once only. It can display in Tabular form only.

  ◆ **Polled**—Repeats polling for the profile according to a specified interval. If you select this option, you can display the SNMP request in a table or a line graph. To display the SNMP replies in a graph, refer to "Graphing SNMP Request Results" on page 336. Selecting this option enables the Poll Interval and Display Style fields.

◆ **Poll Interval**—Changes the polling interval by selecting one of the choices from the drop-down list box.

◆ **Tabular**—Displays the SNMP replies in a table.

◆ **Line Graphs**—Plots the SNMP results in a graph. You can graph scalars and tables with One Row selected. For a detailed description of graphing SNMP results, refer to "Graphing SNMP Request Results" on page 336.

◆ **Attribute Information**—List of attributes that can be selected for SNMP requests.

◆ **Search For**—Specifies a character pattern for the Attribute Choice list. Only attributes matching this pattern are displayed. The default pattern is * (all).

◆ **Category**—Can be one of the following:

  ◆ **Group**—Lists all groups containing at least one scalar attribute.

  ◆ **Table**—Lists all tables.

  ◆ **Scalar**—Lists all scalar attributes.

◆ **Add**—Adds attributes to the Attribute Selection list after selecting them in the Attribute Choices list.

◆ **Remove**—Removes attributes from the Attribute Selection list.

◆ **Row Select**—Selects one or more specific rows in a table. It is enabled only if you have selected the Table category. The Row Selection Criteria dialog box is shown below:
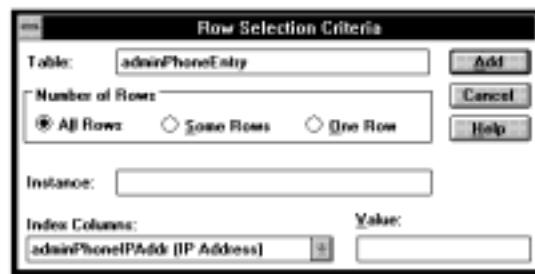
This dialog box contains the following fields:

◆ **Table**—Displays the name of the selected table.

◆ **Number of Rows**—Can be one of the following options:

Option	Explanation
All Rows	Retrieves all rows in a table.
Some Rows	Retrieves a group of rows all sharing the same leading indexes.
One Row	Retrieves the row that matches the indexes you supply.

◆ **Instance**—Displays the concatenation of each entered index value.

◆ **Index Columns/Value**—Activated if you select the option *Some Rows* or *One Row.* You need to select each Index Column in turn and enter the desired value in the Value box.

◆ **Information**—Provides additional information about selected attributes. If you make a selection from the Attribute Choices list and click Information, an Attribute Information window is displayed.

Graphing SNMP Request Results

You can plot the SNMP request results in a graph that displays polled data. Only attributes of type Counter, Integer, and Gauge are plotted. All attributes with type Counter are plotted as rates; attributes with types Integer and Gauge are plotted as current absolute values.

To graph SNMP request results, follow these steps:

Procedure
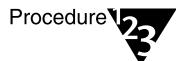
1. **Select an active device.**

2. **Select** *Tools > MIB Browser***.**

   The SNMP MIB Browser window is displayed. A list of existing profiles, along with a description of the selected profile, is displayed in the Profile box.

3. **Select the desired profile and click Edit to bring up the SNMP Profile Editor dialog box.**

4. **Click Polled in the Request Style field.**

5. **Select a polling interval from the Poll Interval drop-down list box.**

6. **Click Line Graphs to create a graph.**

7. **Click Scalar in the Category box.**

8. **Select the scalars you want to graph, and then click Add.**

   The selected scalars move from the Attribute Choices list to the Attribute Selection list.

9. **Click Save.**

10. **Click OK.**

    The SNMP MIB Browser Graph window with the profile values plotted on the graph is displayed.

Note

You can graph only one row of a multiple row table at a time.

The top of the window contains an action bar with four buttons—
Restart, Stop, Option, and Print. These buttons function as follows:

◆ **Restart**—Restarts the operation.

◆ **Stop**—Terminates the current operation.

◆ **Option**—Lets you change the specified community string.

◆ **Print**—Prints the graph.

You can use the buttons on the right edge to display the legend and
X and Y grid lines and to rescale the Y-axis.

chapter **13** *Analyzing Your Network*

With NetWare® LANalyzer® Agent™ software installed on a server on each of your segments, you can use ManageWise® software to help you monitor your network, identify the source of network problems, and maintain optimum performance. This chapter explains the tools provided by ManageWise for analyzing your network performance.

ManageWise provides tools for two kinds of analysis tasks:

◆ Monitoring Segment Performance

   ManageWise collects information about activity on your segments and enables you to see the information broken out into statistics such as utilization and error percentages, both dynamically and over time.

◆ Capturing and Decoding Packets

   ManageWise lets you capture and decode packets, enabling you to analyze your segment by examining the traffic on it.

Monitoring Segment Performance

This section explains how you can use ManageWise to monitor your network and collect information such as the following:

◆ For monitoring network performance, a summary of real-time statistics on all the monitored segments on your network

◆ For monitoring segment performance, detailed real-time and trend statistics for any individual monitored segment

This information is presented in windows containing tables, dials, and graphs. This section also explains how to configure the information displayed in the windows.

Monitoring your segments helps you keep the network operating cost-effectively, consistently, and smoothly. You can use the information you collect in a variety of ways:

◆ To establish a baseline on your network to identify typical traffic loads and control network problems

◆ To analyze real-time performance to help you balance traffic loads among network segments, servers, and routers for a more efficient network

◆ To collect node information to help you focus on specific entities that might be the source of problems

Sometimes a NetWare LANalyzer Agent server must be taken off the network (either for maintenance or because something is wrong with the server). Servers running NetWare LANalyzer Agent 1.1/1.2/1.21 can notify you when nodes you selected for monitoring become inactive (refer to "Monitoring for Inactive Nodes on a Segment" on page 382). To prevent the segment from going unmonitored, choose a different NetWare LANalyzer Agent server on the segment (refer to "Choosing a Remote Monitor" on page 61).

Examining a Summary of All Segments

ManageWise provides a top-level view of all your monitored segments and their performance. Summarizing the performance of your network enables you to keep a picture of its general health. Then, if you detect problems on a segment, you can begin to collect more specific information about the performance of that segment. Refer to "Examining Individual Segments" on page 351 for information about how to use ManageWise to get information about individual segments.

Examining the Network Segments Window

To display the Network Segments window, select *View > All > Network Segments*. Only one instance of the Network Segments window can be open at any time.

The Network Segments window, shown in Figure 13-1, lists the monitored segments on your network and displays statistics for each. Refer to "Configuring the Network Segments Window" on page 350 for information about configuring it to show all segments.

As ManageWise polls segments, messages in the Messages column vary. These messages display the status of the preferred NetWare LANalyzer Agent on the segment.

Note The preferred NetWare LANalyzer Agent is the node you selected to send information about the segment to the ManageWise Console. You select the node in the Database Object Editor. Refer to "Choosing a Remote Monitor" on page 61.

If NetWare LANalyzer Agent is active, there is no message for that polled segment. If NetWare LANalyzer Agent is inaccessible, the corresponding line is disabled. Segments not polled display "Not polled."

Figure 13-1
Network Segments Window

Segment	Type	Speed	Util. %	Packets/s	KBytes/s	Errors/s	Messages
00-00-F6-1A-96-13	Token Ring	16M	1	5	2	0	
#00000002 #00000003	Ethernet	10M	3	129	49	0	
#11223344	Ethernet		0	0	0	0	Not polled
#22334455	Fddi Ring	100M	1	17	9	0	
#33445566	Ethernet	10M	0	0	0	0	Agent not loaded
#44332211	Ethernet		0	0	0	0	Interface not found
#55443322	Ethernet	10M	1	3	3	0	
00-00-C0-6B-34-E4	Ethernet		0	0	0	0	Interface not found
55667788	Token Ring		0	0	0	0	Interface not found

Network Segments : 9 Monitored Segments

The Network Segments window displays one line for each segment, with columns providing the information shown in Table 13-1. The

sampling interval for updating data on monitored network segments is at least 15 seconds.

Table 13-1
Network Segments Window Statistics

Statistic	Explanation
Segment	Segment name or address.
Type	Physical segment type, which is Ethernet, token ring, FDDI, or others (WAN PPP, and so on).
Speed	The speed of the segment, as determined by the speed of the network board that attaches NetWare LANalyzer Agent or the LANtern™ network monitor to the segment and factors such as the cable type of the segment. This column does not show a value if you have not connected to NetWare LANalyzer Agent. This column appears only if you are running NetWare LANalyzer Agent 1.1/1.2/1.21 on at least one server on your network.
Util. %	Average percentage of the bandwidth currently used by all traffic on the segment.
Packets/s	Average number of packets per second currently transmitted on the segment.
KBytes/s	Average number of kilobytes per second currently transmitted on the segment.
Errors/s	Average number of errors per second currently appearing on the segment.
Messages	Status of NetWare LANalyzer Agent on the segment. Refer to Table 13-2 for details.

Table 13-2 lists status and error messages. These messages can appear in the Network Segments window, the NetWare LANalyzer Agent Server dialog box, and the Segment Alarms dialog box. Listed with the messages are explanations and actions you can take to correct possible problems.

Table 13-2
Status and Error Messages for Monitored Segments

Message	Explanation and Action
Agent error	Typically, this message is generated when the NetWare LANalyzer Agent server or LANtern network monitor is out of memory. Rarely, this message is generated because the ManageWise Console sent a malformed SNMP request to the agent or LANtern network monitor.
	If the NetWare LANalyzer Agent server or LANtern network monitor is out of memory, you might have opened several segment-related windows. Segment-related windows in the ManageWise Console require resources on the NetWare LANalyzer Agent server or LANtern network monitor. Try closing some of them. If this does not work, refer to online help for more information about resolving server memory problems. If the server does not appear to be out of memory, verify that the Console has sufficient memory, then restart the ManageWise Console.
Agent not loaded	The NetWare LANalyzer Agent software is not loaded on the server.
	You can use the Remote Console utility in the ManageWise Console to access the server console session. Then, type **LANZ** at the server console prompt.
Available	The NetWare LANalyzer Agent server or LANtern network monitor is responding to the ManageWise Console. This message appears only in the NetWare LANalyzer Agent Server dialog box. In the Network Segments window, the field is blank if the agent or LANtern network monitor is responding.
Cannot turn on promiscuous mode	NetWare LANalyzer Agent failed to turn on promiscuous mode for the interface. There is a problem in the board or the driver, or the server could be running out of resources.
	Try unloading the promiscuous mode driver and reloading it. If this does not work, refer to online help for more information about resolving server memory problems.
Console error	The ManageWise Console failed to send an SNMP request to NetWare LANalyzer Agent or LANtern network monitor, possibly because of insufficient memory on the ManageWise Console.
	Refer to online help for more information about resolving console memory problems.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
Connecting	The ManageWise Console is in the process of connecting to the NetWare LANalyzer Agent server or LANtern network monitor. This is a transient state of the Console. After the connection is established, another status message appears.
Insufficient agent memory	Memory on the NetWare LANalyzer Agent server is insufficient to monitor the interface. Refer to online help for more information about resolving server memory problems.
Interface error	Typically, this error is generated when the NetWare LANalyzer Agent server or LANtern network monitor is out of memory. Rarely, this message is generated because the ManageWise Console sent a malformed SNMP request to the agent or LANtern network monitor.
	If the NetWare LANalyzer Agent server or LANtern network monitor is out of memory, you might have opened several segment-related windows. Segment-related windows in the ManageWise Console require resources on the NetWare LANalyzer Agent server or LANtern network monitor. Try closing some of them. If this does not work, refer to online help for more information about resolving server memory problems. If the server does not appear to be out of memory, verify that the Console has sufficient memory, then restart the ManageWise Console.
Interface initializing	The driver is still initializing on the NetWare LANalyzer Agent server, which is a transient state. This message is very rare because this state lasts only a few milliseconds.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
Interface not found	The ManageWise Console cannot find a particular interface on the NetWare LANalyzer Agent server or LANtern network monitor. Possible reasons for this problem are as follows:

◆ The LAN driver for the adapter related to this interface is not loaded or has been updated.

◆ The network board was removed from the NetWare LANalyzer Agent server or exchanged for a new one.

◆ A new NetWare LANalyzer Agent server is added to the network and it is assigned an IPX™ or IP address that was used previously.

◆ A LANtern network monitor was replaced and the IP address assigned to the new monitor is the same as the LANtern network monitor that was removed.

Select the appropriate action:

◆ If the LAN driver is not loaded, load it. You can use the Remote Console utility in the ManageWise Console to access the server console session. Refer to the vendor's documentation for information about what command to use to load the driver.

◆ If you removed or changed a network board, wait until NetExplorer™ software completes its next cycle and, subsequently, NetExplorer Manager runs on the ManageWise Console. NetExplorer detects that a network board is removed or changed and updates the ManageWise database accordingly. If you do not want to wait for NetExplorer to run, you can update the information yourself in the Database Object Editor.

◆ If you assigned a previously used IPX or IP address to a new NetWare LANalyzer Agent server, reassign it an IPX or IP address that was not assigned previously. Then run NetExplorer again and check to see that NetExplorer handles this properly. Alternatively, use the Database Object Editor to change the IPX address.

◆ If you assigned a previously used IP address to a new LANtern network monitor, use the NXPCON utility on the NetExplorer Server to change the LANtern name in the NXPLANZ discovery option. Then unload NXPLANZ and reload it.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
Interface status unknown	An unknown error occurred when the ManageWise Console tried to gather information from the NetWare LANalyzer Agent or LANtern network monitor. This error should not occur under typical conditions.
	Free memory on the ManageWise Console. If another ManageWise Console can communicate with the NetWare LANalyzer Agent or LANtern network monitor, the problem is probably a console problem.
	If no other console can communicate with the ManageWise Console, the problem is probably with the NetWare LANalyzer Agent or LANtern network monitor. You might have opened several segment-related windows. Segment-related windows in the ManageWise Console require resources on the NetWare LANalyzer Agent server or LANtern network monitor. Try closing some of them. If this does not work, refer to online help for more information about resolving server memory problems.
No response	The NetWare LANalyzer Agent or LANtern network monitor is not responding to SNMP requests or pings. Either the agent or LANtern network monitor is not alive or the ManageWise Console cannot reach it. Possibly the network cabling is down, a router is down, or NetWare is not functioning.
	Check whether the NetWare LANalyzer Agent or LANtern network monitor is up and running, that the cabling is functioning, and that NetWare is functioning.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
No SNMP response	The NetWare LANalyzer Agent server or LANtern network monitor is responding to pings but not to SNMP requests. Possible reasons for this problem are as follows: ◆ The SNMP Agent is not loaded on the server. ◆ There is a mismatch between the community parameters configured on the target server or LANtern network monitor and the GET community string configured in the ManageWise database. ◆ The timeout value (the number of seconds between retry attempts) configured in the ManageWise Console for the SNMP GET and SET operations to the target server or LANtern network monitor is too small. To resolve the problem, try the following: ◆ If the SNMP Agent is not loaded, use the Remote Console utility in the ManageWise Console to access the server console session. Then enter `LOAD SNMP {community name option}` at the server console prompt to load the agent, or use the INETCFG utility. To use the INETCFG utility, load INETCFG, and then select *Manage Configuration > Configure SNMP Parameters*. ◆ Try increasing the timeout value. If you explicitly configured the community strings for the target node in the SNMP Options Setup dialog box (*Configure > SNMP Options*), change the timeout value in that dialog box. If you are using the global values for community strings, configured in the SNMP Options dialog box (*Configure > Global Preferences > SNMP Options*), check the timeout value in that dialog box.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
No statistics	A statistics table entry cannot be found on NetWare LANalyzer Agent, probably because the agent is not monitoring that interface. This error message appears in the following circumstances: ◆ NetWare LANalyzer Agent 1.0 is running on the segment. (This is the most likely cause.) We recommend that you upgrade NetWare LANalyzer Agent to version 1.21. To upgrade NetWare LANalyzer Agent to version 1.21, install ManageWise 2.6 or, if you want to upgrade only the agent software, download the version 1.21 upgrade (NWLANZ.EXE) from the ManageWise section at http://www.novell.com/download. ◆ The interface cannot be monitored because the driver is not supported. The driver must support promiscuous mode and the raw send feature. If the adapter is not using a promiscuous mode driver, install one on the server. Check NetWire for information regarding availability of the latest promiscuous mode drivers. You might have to contact your adapter vendor for the appropriate driver. If the adapter is using a promiscuous mode driver, try unloading the driver and reloading it. If this does not work, refer to online help. ◆ You disabled monitoring on the agent.
Not monitored	The segment is not an Ethernet, a token ring segment, or a FDDI segment, or no NetWare LANalyzer Agent or LANtern network monitor is installed on the segment. This message appears in the Network Segments window only, and only if the window is configured to show all segments (both monitored and unmonitored). In the Segment Alarms dialog box, "Segment not monitored" has the same meaning as "Not monitored." If you want the Ethernet, token ring, or FDDI segment to be monitored, install NetWare LANalyzer Agent 1.21 on a server on the segment. NetWare LANalyzer Agent 1.21 is included with ManageWise 2.6 or available from Electronic Software Distribution (ESD) as an upgrade to version 1.20.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
Not polled	The ManageWise Console is not querying NetWare LANalyzer Agent or LANtern network monitor on the segment for statistics because polling for this segment is set to Stop. If you want statistics for the monitored segment, start polling on the segment. In the Network Segments window, select the segments you want to be polled, and then click *Start Polling*. In other ManageWise windows that require that the segment be polled to obtain data, you are prompted to start polling if polling has not been started already. When you select a segment for polling, ManageWise retains that setting. Therefore, when you restart the ManageWise Console, polling starts again for the segments that you selected for polling.
Not promiscuous mode driver	The driver is not a promiscuous mode driver. NetWare LANalyzer Agent requires promiscuous mode to function properly. Install a promiscuous mode driver on the server. Check NetWire for information regarding availability of the latest promiscuous mode drivers. You might have to contact your adapter vendor for the appropriate driver.
Not raw send driver	The driver is not a raw send driver. NetWare LANalyzer Agent requires an adapter driver that supports the raw send feature. Install an adapter driver that supports raw send on the server.
Obtaining data	The ManageWise Console successfully communicated with the NetWare LANalyzer Agent server or LANtern network monitor. The Console sent (or is waiting to send) additional SNMP requests to obtain statistics. (This message appears only in the Network Segments window.)
Segment not monitored	The segment is not an Ethernet, a token ring segment, or a FDDI segment, or no NetWare LANalyzer Agent or LANtern network monitor is installed on the segment. This message appears in the Network Segments window only, and only if the window is configured to show all segments (both monitored and unmonitored). In the Segment Alarms dialog box, "Segment not monitored" has the same meaning as "Not monitored." If you want the Ethernet, token ring, or FDDI segment to be monitored, install NetWare LANalyzer Agent 1.21 on a server on the segment. NetWare LANalyzer Agent 1.21 is included with ManageWise 2.6 or available from the ManageWise section at http://www.novell.com/download.as an upgrade to version 1.20.

Table 13-2 *continued*
Status and Error Messages for Monitored Segments

Message	Explanation and Action
Unreachable	When the NetWare LANalyzer Agent server was pinged, this message was returned. ManageWise does not know how to send a packet to the target. That is, none of the routers adjacent to the ManageWise Console can forward packets to the target. This can happen if the target router or server is down or if any of the intermediate routers between the ManageWise Console and the target is down.
	To resolve the problem, do one of the following:
	◆ If the target is a router or server, determine if it is down.
	◆ If the server or router is not down, determine whether any of the routers between the ManageWise Console and the target network is down.
	◆ If the NetWare LANalyzer Agent server or a router on the path to the server is not down, try restarting the ManageWise Console to reload drivers.
Unsupported pipelined adapter	The adapter is a pipelined adapter and is not supported by NetWare LANalyzer Agent. If the adapter allows you to switch from pipelined mode to non-pipelined mode, do so. If the adapter cannot switch modes, use a non-pipelined adapter for NetWare LANalyzer Agent transactions.
Unsupported RNS interface	This message is informational. This is a Remote Node Service (RNS) interface, which NetWare LANalyzer Agent does not support (because it is not a promiscuous mode driver). However, when NetExplorer discovers RNS interfaces, it connects them to Ethernet segments on ManageWise maps. Note that the Database Object Editor might show "Unknown" for an RNS interface. If you want, you can change the interface type manually.

Configuring the Network Segments Window

You can configure the Network Segments window to show only the monitored segments (those with NetWare LANalyzer Agent or LANtern network monitor attached) or to show all segments on the network.

◆ When you show all monitored segments, the window title indicates "Network Segments: *x* Monitored Segments," where *x* is the number of segments with NetWare LANalyzer Agent installed. If your NetWare LANalyzer Agent can monitor multiple segments, the number *x* might be larger than the number of copies of NetWare LANalyzer Agent software on your network.

◆ When you show all segments, including those without NetWare
  LANalyzer Agent, the window title indicates "Network Segments:
  x Segments," where *x* is the total of all discovered segments. In the
  Messages column, the segments without NetWare LANalyzer
  Agent indicate "Not monitored."

To configure the window, follow these steps:

Procedure
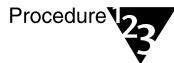
**1. With the Network Segments window displayed and active,
    select *Configure > Active Window*.**

The Configure Network Segments window is displayed.

**2. Click the Show all segments or Show monitored segments
    option button.**

The default setting is to show only monitored segments. To change
the default, click the Show all segments option button, then click
the Save as default check box.

3. Click OK.

Examining Individual Segments

While monitoring your network, you might discover a problem or want
to see more information about an individual segment. To help you do
so, ManageWise lets you perform the following operations:

◆ Summarizing the Performance of a Single Segment on page 352

◆ Examining the Most Active Nodes on a Segment on page 353

◆ Examining Conversations (Traffic) Between Nodes on page 358

◆ Examining Trend Data for a Segment on page 361

◆ Examining Segments on page 374

◆ Examining Segment Information on page 380

◆ Monitoring for Inactive Nodes on a Segment on page 382

◆ Capturing and Decoding Packets on page 384

Summarizing the Performance of a Single Segment

ManageWise provides a real-time overview of the performance of any individually monitored segment on your network. This overview, which is displayed in the Network Dashboard™ window shown in Figure 13-2, is useful if you want to troubleshoot a segment.
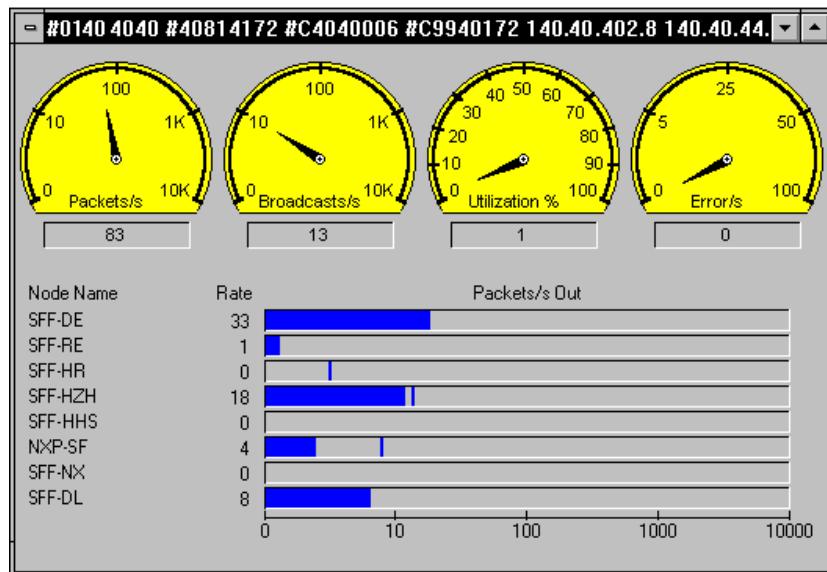
The window title shows the name of the segment. Below the title, the window shows four gauges, which display the following four real-time statistics for the segment:

◆ **Packets/s**—Number of packets per second currently transmitted on the segment.

◆ **Broadcasts/s**—Number of broadcast packets per second currently transmitted on the segment (a broadcast packet is sent to all addresses on the segment).

◆ **Utilization %**—Percentage of maximum network capacity currently consumed by packet traffic on the segment.

◆ **Error/s**—Number of error packets per second currently transmitted on the segment.

Gauge statistics are updated every five seconds. The gauge needles move according to rate and percentage changes. The numeric value of each gauge is displayed below the gauge.

To display the Network Dashboard window, follow these steps:

Procedure 23

1. **Select a segment in the Network Segments window, the internetwork map, or a segment map.**

   The line containing the segment is highlighted, and the action bar buttons you can use become active.

2. **Click the Network Dashboard button.**

   Alternatively, you can double-click the line of a monitored segment on the Network Segments window, or you can select a segment from an internetwork map, and then select *Performance > Dashboard*.

   The Network Dashboard window opens.

Examining the Most Active Nodes on a Segment

You can use ManageWise to determine the most active nodes on a segment for a wide range of performance statistics. This is useful if you want to discover which node is generating the most traffic based on a particular statistic. For example, you might want to find the heaviest source of broadcast traffic.

ManageWise provides two windows for discovering the active nodes: the Top Nodes graph and the Stations table. These are explained in the following sections.

Examining the Top Nodes Graph

The Top Nodes graph is in the lower portion of the Network Dashboard window. It displays the top eight nodes, based on a selected statistic, for the selected segment. If you want to see the top eight nodes on another segment, you can select another segment in the Network Segments window and open another Network Dashboard window.

Statistics are updated every 5 seconds. Every 60 seconds, the table is sorted again and the new top users are displayed. At this point, new nodes might be added to the list and existing ones might drop out. The default statistic is packets out per second and can be configured as explained in the following section.

Note ▼ Errors per minute, Broadcasts per minute, and Multicasts per minute are updated every 60 seconds rather than every 5 seconds.

Configuring the Top Nodes Graph

You can configure the Network Dashboard window to display or disable the Top Nodes graph and, if it is displayed, to change the statistic.

To configure the Network Dashboard window, follow these steps:

Procedure ▼
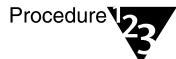
1. **With a Network Dashboard window displayed and active, select** *Configure > Active Window.*

   The Configure Network Dashboard dialog box is displayed.

2. **If you want to reconfigure the Top Nodes graph to base the top nodes on a different statistic, click the Select top nodes by: option button in the Rate Selection box, and select the statistic you want from the drop-down list box.**

   You can choose one of these statistics:

   ◆ **Packets in/s**—Packets per second received by a node.

   ◆ **Packets out/s**—Packets per second transmitted by a node.

   ◆ **Bytes in/s**—Bytes per second received by a node.

   ◆ **Bytes out/s**—Bytes per second transmitted by a node.

   ◆ **Errors/min**—Errors per minute transmitted by a node.

   ◆ **Broadcasts/min**—Broadcast packets per minute transmitted by a node.

   ◆ **Multicasts/min**—Multicast packets per minute transmitted by a node.

3. **If you do not want to display the Top Nodes graph, select the Disable top nodes graph option button.**

4. **If you want to save the new configuration as the default, click the Save as default check box at the bottom of the window.**

   The next time you open the window, the new configuration is displayed.

5. **Click OK.**

Examining the Top 20 Stations Window

The Top 20 Stations window, shown in Figure 13-3, lists the top 20 nodes sorted by packets out, per second. If there are fewer than 20 nodes, all the nodes are listed. The next section explains how to change the statistic on which the table is sorted.

Figure 13-3
Top 20 Stations Window

Node	Util. %	Pkts/s Out	Bytes/s Out	Errors/s	Pkts/s In	Bytes/s In	Broa
SJF-PRD	1	12	2,795	0	10	1,476	
SJF-71-EDL	1	8	2,022	0	6	1,173	
800014980849	1	1	43	0	1	32	
0880D681B8F4	1	1	54	0	1	37	
800014938523	1	1	11	0	1	11	
00001D0E8923	1	1	35	0	0	0	
8000077E7A00	1	1	52	0	1	33	
SJF-ED	1	1	6	0	1	9	
91891914425E	0	0	0	0	0	0	
TSM	0	0	0	0	0	0	
SJF-PRO	1	1	38	0	0	0	
SJF-ED-P	1	1	40	0	1	6	
80001B19A146	0	0	0	0	0	0	
0880D461BA46	0	0	0	0	1	6	
ATalk	0	0	0	0	1	347	
9180C2002014	0	0	0	0	0	0	
SJF-ED-G	0	0	0	0	0	0	
DEC_IcI_B	0	0	0	0	2	66	
98981B199898	0	0	0	0	0	0	
TRAIN	1	2	1,031	0	2	120	

Window title: #4001 4040 130.40.40.0 - Top 20 Stations - Packets/s Out

The window title shows the name or address of the selected segment, and the statistic used to select the top 20 nodes. The columns show the statistics explained in Table 13-3.

Table 13-3
Top 20 Stations Statistics

Statistic	Explanation
Node	Name of the node (or address, if the name is not in the ManageWise database).
Util. %	Percentage of maximum network capacity consumed by packets sent by a node.
Pkts/s Out	Packets per second transmitted by a node.
Bytes/s Out	Bytes per second transmitted by a node.
Errors/s	Errors per second transmitted by a node.
Pkts/s In	Packets per second received by a node.
Bytes/s In	Bytes per second received by a node.
Broadcasts/s	Broadcast packets per second transmitted by a node.
Multicasts/s	Multicast packets per second transmitted by a node (packets transmitted to a specific group of nodes).
Protocols	Types of protocols used by a node.
First Transmit	Date and time a node first transmitted since NetWare LANalyzer Agent was started.
Last Transmit	Date and time a node last transmitted since NetWare LANalyzer Agent was started.
MAC address	Physical (MAC) address of a node.

Statistics are updated every 5 seconds. Every 60 seconds, the table is sorted again and new top users are displayed. At this point, new nodes might be added to the list and existing ones might drop out.

To display the Stations table window, follow these steps:

1. **Select a segment from the Network Segments window, an internetwork map, or a segment map.**

   The segment is highlighted and, in the Network Segments window, the action bar buttons you can use become active.

2. **Display the Stations table window in either of these ways:**

   2a. **If you selected your segment from the Network Segments window, click the Stations button.**

   2b. **If you selected your segment from an internetwork map, select *Performance > Stations*.**

   The Stations table is displayed.

If you want to see the activity for specific nodes on a segment, you can create a Stations table for those nodes by first selecting them from an existing Stations table window, from a segment map, from a Ring Stations table, or from a Conversations table. Then, select *Performance > Stations* to display the window.

Configuring the Stations Table Window

You can configure the Stations table to display only the top 20 nodes or all nodes and to select the statistics used to select the top 20 nodes.

Important

If you display all nodes, more time and network bandwidth are used.

To configure the Stations table, follow these steps:

1. **With a Stations table displayed and active, select *Configure > Active Window*.**

   The Configure Stations Window dialog box is displayed.

   If you want to see statistics about only the top 20 nodes, click the Select top nodes by: option button in the Settings box and choose a statistic from the drop-down list box.

These statistics are available:

- ◆ **Packets In/s**—Packets per second received by a node.

- ◆ **Packets Out/s**—Packets per second transmitted by a node.

- ◆ **Bytes In/s**—Bytes per second received by a node.

- ◆ **Bytes Out/s**—Bytes per second transmitted by a node.

- ◆ **Errors Out/s**—Errors per second transmitted by a node.

- ◆ **Broadcasts/s**—Broadcast packets per second transmitted by a node.

- ◆ **Multicasts/s**—Multicast packets per second transmitted by a node.

- ◆ **Utilization %**—Percentage of maximum network capacity consumed by packets sent by a node.

2. **If you prefer to see statistics for all nodes, click the Show all nodes option button in the Settings box.**

   Keep in mind, however, that more time and network traffic are then required to obtain and display statistics.

3. **If you want to save the new configuration as the default, click the Save as default check box at the bottom of the window.**

4. **Click OK.**

Examining Conversations (Traffic) Between Nodes

ManageWise provides real-time data about all the network traffic between a selected node and one or more other nodes. The data, which is displayed in the Conversations table shown in Figure 13-4, can be used to determine specific information about node communication. For example, it can show which nodes communicate with a router or server, determine the load on a server, or examine the traffic flowing to or from a node that is reporting difficulties.

You can select either one or two nodes from a map or from the Stations table before displaying the Conversations table.

◆ If you select one node, statistics are displayed for all other nodes that converse with the selected node.

◆ If you select two nodes, only one row is displayed in the Conversations table with statistics for traffic between the two nodes.

Figure 13-4 shows a Conversations table for one node, SFF-NM.

Figure 13-4
Conversations Table Window

Node	% Pkt Load	% Byte Load	Pkts/s In	Pkts/s Out	Bytes/s In	Bytes/s Out	Pkts In
TRAIN	0	0	0	0	0	0	
00001B00DF3F	1	1	1	0	8	0	
0020AF8DA5A6	0	0	0	0	0	0	
0080D301B8BA	3	1	1	1	24	32	1
0080D301BA06	4	1	1	1	27	38	1
0080D301BA30	1	1	1	1	6	6	
0080D302E306	3	1	1	1	38	33	1
SJF-71-EDL	67	73	10	10	2,595	2,681	39
0800077E7A5F	4	2	1	1	30	51	1
080014949491	2	1	1	1	9	15	
080014946849	3	1	1	1	26	33	
ATalk	2	5	1	0	345	0	1
DEC_lcl_B	4	1	2	0	65	0	3
SJF-ED	0	0	0	0	0	0	
Broadcast	10	20	3	0	1,407	0	12
SJF-ED-L	2	1	1	0	29	0	
0900070070D5	1	1	1	0	4	0	
SJF-ED-C	1	1	0	1	0	4	

The title bar shows the node for which statistics are shown. The columns display the statistics shown in Table 13-4, which are updated every 5 seconds.

Note ▼ The Conversations table lists the percentage of traffic that each node contributes to one node's load. However, due to sample skewing (samples not taking place at the same time) and rounding up of statistics, the numbers in the columns do not always add up to 100%.

Table 13-4
Conversations Table Statistics

Statistic	Explanation
Node	Name of the node (or address, if the name is not in the ManageWise database) communicating with the node in the title bar.
% Pkt Load	Percentage of the packets sent to or from the node in the title bar that were sent to or from a node.
% Byte Load	Percentage of the bytes sent to or from the node in the title bar that were sent to or from a node.
Pkts/s In	Packets per second received by a node from the node in the title bar.
Pkts/s Out	Packets per second transmitted by a node to the node in the title bar.
Bytes/s In	Bytes per second received by a node from the node in the title bar.
Bytes/s Out	Bytes per second transmitted by a node to the node in the title bar.
Pkts In	Number of packets received by a node from the node in the title bar since the window opened.
Pkts Out	Number of packets transmitted by a node to the node in the title bar since the window opened.
KBytes In	Total kilobytes received by a node from the node in the title bar since the window opened.
KBytes Out	Total kilobytes transmitted by a node to the node in the title bar since the window opened.
Protocols	Protocol packet types used by a node in this conversation.
First Transmit	Date and time that a node first transmitted on the network since NetWare LANalyzer Agent was loaded.
Last Transmit	Date and time that a node last transmitted since NetWare LANalyzer Agent was loaded.
MAC Address	Physical (MAC) address of a node.

Refer to *ManageWise 2.6 Setup Guide* for more information on sorting the table entries, rearranging the columns, or exporting the data from this table.

To examine node conversations, follow these steps:

Procedure

1. **Select one or two nodes on an Ethernet, token ring, FDDI map, the Stations table, the Ring Stations window, FDDI Stations window or an existing Conversations table.**

   The icon or line becomes highlighted.

2. **Select *Performance > Conversations*.**

   Alternatively, you can double-click one node from the Stations table, Ring Stations window, or FDDI Ring Stations window to show all conversations with that node.

Examining Trend Data for a Segment

The Segment Trends window displays graphs of segment performance trends. The time periods over which you can view trend data depends on the version of NetWare LANalyzer Agent installed on the segment, as follows:

◆ **If NetWare LANalyzer Agent 1.1/1.2/1.21 is installed on the segment's preferred NetWare LANalyzer Agent server**—You can view current trends, gathered every 30 seconds over the last hour. You can also view historical trends, displayed over hourly, daily, weekly, monthly, or yearly periods.

Note   When multiple nodes running NetWare LANalyzer Agent are located on the same segment, the node that you select in the NetWare LANalyzer Agent server dialog box as the node to send information about the segment to the ManageWise Console is the preferred NetWare LANalyzer Agent server.

◆ **If NetWare LANalyzer Agent 1.1/1.2/1.21 is installed on the network but not on the segment's preferred NetWare LANalyzer Agent server**—You can view only current trends for this segment. Current trends are gathered every 30 seconds over the last hour. We recommend that you select a server with NetWare LANalyzer Agent 1.1/1.2/1.21 as the segment's preferred server.

◆ **If all NetWare LANalyzer Agent software installed on the network is version 1.0**—You can view current trends (past hour) and trends for the past day.

Note ▼ We recommend that you upgrade NetWare LANalyzer Agent servers to version 1.21 because of the significant additional functionality and improved performance that version 1.21 provides. To upgrade NetWare LANalyzer Agent to version 1.21, install ManageWise 2.6 or, if you want to upgrade only the agent software, download the version 1.21 upgrade (NWLANZ.EXE) either from the ManageWise section at http://www.novell.com/download or from Electronic Software Distribution (ESD).

You can use trend information to create a baseline of typical activity on segments. Having a baseline helps you set appropriate thresholds for segment alarms and plan maintenance activities and backups. Additionally, if problems occur on the segment, you can compare the typical traffic level against the traffic level at the time of the problem, which might help you discover the cause of the problem.

Ethernet default statistics displayed are total packets (shown in red), good packets (shown in gray), and error packets (shown in yellow). The token ring default statistic displayed is total packets. The window title shows the name of the segment and the statistics currently displayed. The FDDI ring default statistic displayed is total packets. The window title shows the name of the segment and the statistics currently displayed.

Examining the Segment Graph Window

Trend data for a segment is displayed in the Segment Graph window, shown in Figure 13-5 and Figure 13-6.

Figure 13-5
Segment Graph Window (NetWare LANalyzer Agent 1.21)
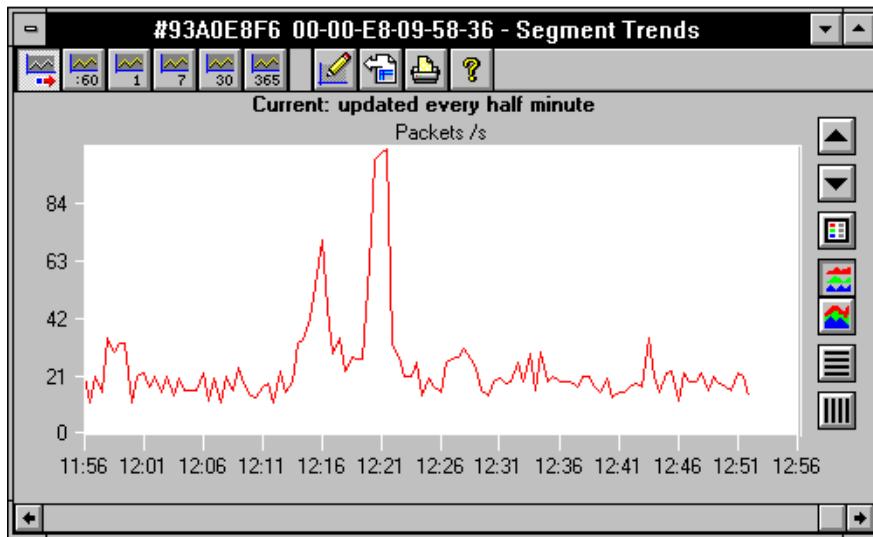
Figure 13-5 shows a Segment Graph window for a network that has NetWare LANalyzer Agent 1.1/1.2/1.21 installed. (Version 1.21 is installed as part of ManageWise 2.6.) The action bar at the top of the window enables you to change the time span of the trend you view, to change statistics you view, to export data to a file, and to print the Segment Graph window to a printer. A description of the action bar buttons, described from the left-most button to the right-most, follows:

◆ **Current Trend**—Displays a current trend graph. The default sampling time for this graph is once every minute. This graph updates in real time.

Note   Although the graph has a scroll bar, do not rely on a current trend graph to show you data previously gathered (within the last week, for example). Data is constantly gathered and written over. The data you want to view might be gone. View one of the historical trend graphs to see previously gathered data.

◆ **Hourly Trend**—Displays a historical graph of the selected trend with a time span of one hour.

◆ **Daily Trend**—Displays a historical graph of the selected trend with a time span of one day.

◆ **Weekly Trend**—Displays a historical graph of the selected trend with a time span of one week.

◆ **Monthly Trend**—Displays a historical graph of the selected trend with a time span of one month.

◆ **Yearly Trend**—Displays a historical graph of the selected trend with a time span of one year.

Note Historical trends, such as hourly, daily, weekly, monthly, and yearly trends are available only when NetWare LANalyzer Agent 1.1/1.2/1.21 is installed on the segment's preferred NetWare LANalyzer Agent server.

◆ **Configure Active Window**—Opens the Configure Segment Graph dialog box. Using this action bar button, you can configure the Segment Graph window to display different statistics, as explained in "Configuring a Segment Graph Window" on page 367.

◆ **Export**—Copies the information in the Segment Trends window to a file. Refer to *ManageWise 2.6 Setup Guide* for detailed instructions.

◆ **Print**—Prints the information listed in the Segment Trends window to a printer.

◆ **Help**—Displays online help. This is equivalent to pressing the F1 key.

The graph control buttons, located at the side of the graph, are described in the online help.

Figure 13-6
Segment Graph Window (NetWare LANalyzer
Agent 1.0 only)
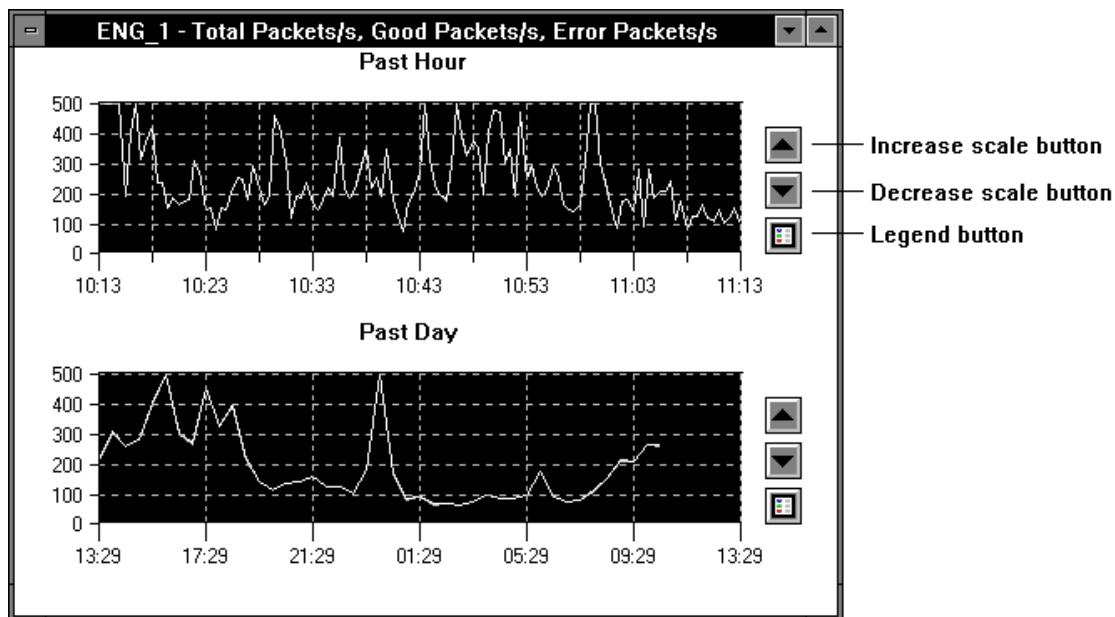
Figure 13-6 shows a Segment Graph window for networks that only have NetWare LANalyzer Agent 1.0. The window title shows the name of the segment and which statistics are being displayed. Below it are two labeled graphs:

◆ **Past Hour**—Values at 30-second intervals.

◆ **Past Day**—Values at 30-minute intervals.

The graphs show the default statistics for Ethernet/token ring/FDDI segments:

◆ **Ethernet**—Default statistics are total packets, good packets, and error packets.

◆ **Token ring**—Default statistic is total packets.

◆ **FDDI**—Default statistic is total packets.

You can configure the Segment graph to display different statistics, as explained in the next section, "Configuring a Segment Graph Window."

To display the Segment Graph window, follow these steps:

Procedure

1. **Select a segment from the Network Segments window, an internetwork map, or a segment map.**

   The segment is highlighted and, in the Network Segments window, the action bar buttons you can use become active.

2. **Display the Segment graph.**

   You can display the Segment graph by clicking the Segment Trends action bar button or by selecting *Performance > Segment Trends.*

   The Trends graph is displayed.

To see a Segment graph for a statistic shown in a Network Dashboard gauge, double-click the gauge. The Segment graph appears, configured to display the statistic shown by the gauge.

To the right of the Segment graph are three control buttons that you can use to modify the display. For more information about these buttons, refer to the online help.

Configuring a Segment Graph Window

You can configure the Segment Graph window for Ethernet, token ring, or FDDI segments to choose which statistics to display. Figure 13-7 shows the Configure Segment Graph dialog box for an Ethernet segment.

**Figure 13-7
Ethernet Configure
Segment Graph
Dialog Box**
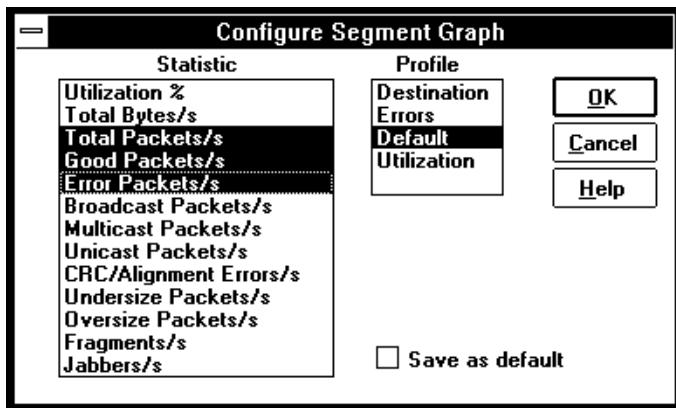
The Statistic box lets you examine the following Ethernet statistics:

◆ **Utilization %**—Percentage of maximum network capacity consumed by all packets.

◆ **Total Bytes/s**—Total bytes per second transmitted on this segment.

◆ **Total Packets/s**—Total packets per second transmitted on this segment.

◆ **Good Packets/s**—Total good packets per second transmitted on this segment.

◆ **Error Packets/s**—Total error packets per second transmitted on this segment.

◆ **Broadcast Packets/s**—Average number of packets per second sent to the broadcast address FF-FF-FF-FF-FF-FF; broadcast messages typically consist of general requests for information or transmission of status information to all nodes.

◆ **Multicast Packets/s**—Average number of packets per second sent to a selected group of addresses.

◆ **Unicast Packets/s**—Average number of packets per second sent to a single recipient.

◆ **CRC/Alignment Errors/s**—Average number of cyclic redundancy check (CRC) errors per second; these packets are of legal size but have a faulty Frame Check Sequence (FCS) and Alignment Errors per second.

◆ **Undersize Packets/s**—Average number of undersized packets observed per second; undersized packets are shorter than 64 bytes.

◆ **Oversize Packets/s**—Average number of oversized packets observed per second; oversized packets contain more than 1518 bytes, including the FCS.

◆ **Fragments/s**—Average number of fragments observed per second; fragments are packets that contain less than 64 bytes and have a faulty FCS. They are typically a result of collisions.

◆ **Jabbers/s**—Average number of jabber packets observed per second; jabber consists of packets that contain more than 1518 bytes and have a faulty FCS.

Figure 13-8 shows a token ring Configure Segment Graph dialog box.

Figure 13-8
Token Ring
Configure Segment
Graph Dialog Box
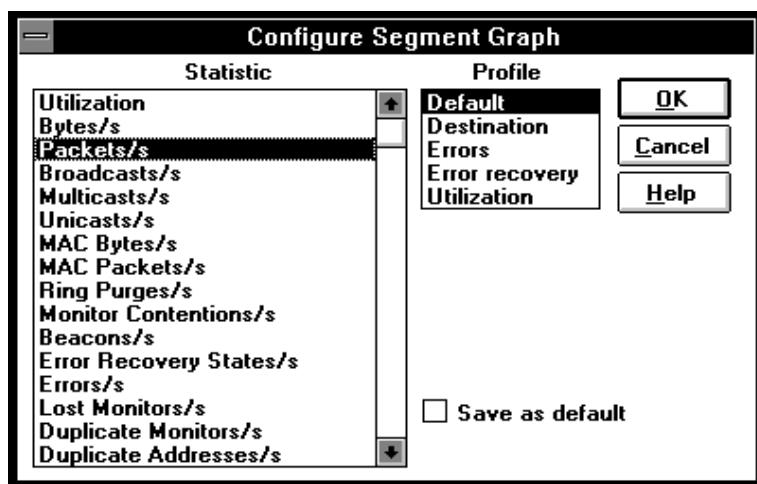
The Statistic box lets you examine the following token ring statistics (you can scroll the list to see all the statistics):

◆ **Utilization**—Percentage of maximum network capacity used by all packets.

◆ **Bytes/s**—Average number of bytes observed per second.

◆ **Packets/s**—Average number of packets observed per second.

◆ **Broadcasts/s**—Average number of packets per second sent to the broadcast addresses FF-FF-FF-FF-FF-FF and C0-00-FF-FF-FF-FF; broadcast messages typically consist of general requests for information or transmission of status information to all nodes.

◆ **Multicasts/s**—Average number of packets per second sent to a selected group of addresses.

◆ **Unicasts/s**—Average number of packets per second sent to a single destination.

◆ **MAC Bytes/s**—Average number of MAC bytes observed per second; MAC packets are used to manage the ring.

◆ **MAC Packets/s**—Average number of MAC packets observed per second; MAC packets are used to manage the ring.

◆ **Ring Purges/s**—Average number of times per second the ring entered the purge state from normal ring state.

◆ **Monitor Contentions/s**—Average number of monitor contentions observed per second; these packets are transmitted by all active nodes when no Active Monitor is detected on the ring.

◆ **Beacons/s**—Average number of beacons observed per second; a node transmits these packets when it detects a hard failure upstream of itself.

◆ **Error Recovery States/s**—Average number of error recovery packets per second; this total combines the ring purge, monitor contention, and beacon packets.

◆ **Errors/s**—Average number of all types of error packets per second; this total combines packets indicating lost monitor, duplicate

monitor, duplicate addresses, ring poll failures, line errors, internal errors, burst errors, AC errors, abort delimiter errors, lost frames, receive congestion errors, frame copied errors, frequency errors, and token errors.

◆ **Lost Monitors/s**—Average number of monitor error packets per second received by the node.

◆ **Duplicate Monitors/s**—Average number of duplicate monitor errors observed per second; a duplicate monitor error occurs when an Active Monitor detects another Active Monitor on the ring.

◆ **Duplicate Addresses/s**—Average number of times a node reported another node using its own address per second.

◆ **Ring Poll Failures/s**—Average number of ring poll failure MAC packets observed per second.

◆ **Line Errors/s**—Average number of line errors observed per second; these packets are of legal size but have a faulty FCS and do not end on an 8-bit boundary.

◆ **Internal Errors/s**—Average number of internal errors observed per second; these errors generally indicate a network adapter board failure.

◆ **Burst Errors/s**—Average number of burst errors observed per second; this error indicates that a node detects the absence of transitions for the required time.

◆ **AC Errors/s**—Average number of AC errors observed per second; this error is reported when an intended recipient of a packet fails to mark it as received or flags an error on it.

◆ **Abort Delimiter Errors/s**—Average number of abort delimiter errors observed per second; this error indicates that a node aborts a transmission.

◆ **Lost Frames/s**—Average number of lost frame errors observed per second on the network.

◆ **Receive Congestion Errors/s**—Average number of receive congestion errors observed per second; this error indicates that a

node recognizes a frame addressed to its address but has no available buffer space.

◆ **Frequency Errors/s**—Average number of frequency errors observed per second; this error indicates that a token ring clock on a node differs too much from the clock on the Active Monitor.

◆ **Token Errors/s**—Average number of token errors observed per second; this error indicates that a token has become corrupted or the Active Monitor did not see a new frame in the required amount of time.

Figure 13-9 shows the FDDI Configure Segment Graph dialog box for a FDDI segment.
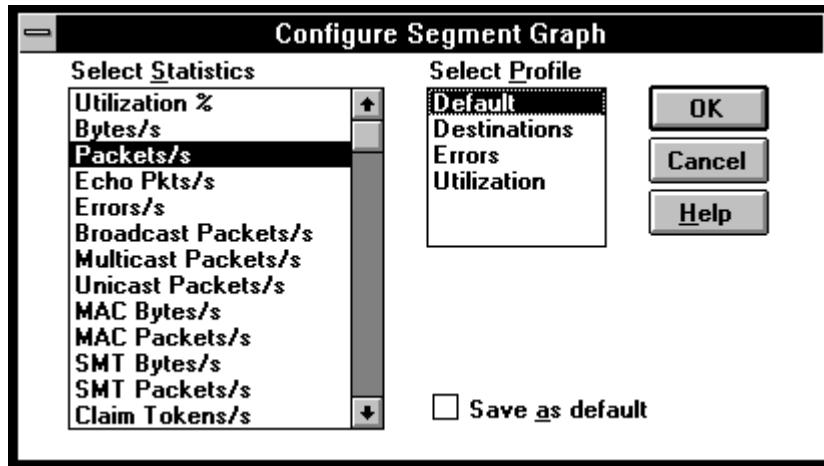
The Statistic box lets you examine the following FDDI statistics:

◆ **Utilization%** —Percentage of maximum network capacity consumed by all packets.

◆ **Bytes/s**—Average number of bytes observed per second.

◆ **Packets/s**—Average number of packets observed per second.

◆ **Echo Pkts/s**—Average number of echo frames received on the network per second.

◆ **Errors/s**—Average number of all types of error packets per second; this total combines packets indicating beacons, ring wraps, frame copied errors, elasticity buffer overflow errors, CRC errors, lost frames, undersize packets, and oversize packets.

◆ **Broadcast Packets/s**—Average number of packets per second sent to the broadcast address FF-FF-FF-FF-FF-FF; broadcast messages typically consist of general requests for information, or transmission of status information to all nodes.

◆ **Multicast Packets/s**—Average number of packets per second sent to a selected group of addresses.

◆ **Unicast Packets/s**—Average number of packets per second sent to a single recipient.

◆ **MAC Bytes/s**—Average number of MAC bytes observed per second; MAC packets are used to manage the ring.

◆ **MAC Packets/s**—Average number of MAC packets observed per second; MAC packets are used to manage the ring.

◆ **SMT Bytes/s**—Average number of good SMT octets received per second on the network.

◆ **SMT Packets/s**—Average number of good SMT packets received per second on the network.

◆ **Claim Tokens/s**—Average number of times that the ring enters the claim token state from normal ring state or ring purge state per second.

◆ **Ring Wraps/s**—Average number of times a wrap around condition has been detected at this interface per second. This entry does not indicate the number of times the ring has actually wrapped around. It indicates the number of times the ring has wrapped around this physical path.

◆ **Elasticity Buffer Errors/s**—Average number of elasticity buffer overflow errors reported per second by this station per second. This is due to the difference in the clock frequency of the transmitting and receiving stations.

◆ **CRC Errors/s**—Average number of frames with CRC errors received per second on the network.

◆ **Undersize Packets/s**—Average number of packets received per second that were between 0 and 10 octets in length inclusive, excluding framing bits but including FCS octets.

◆ **Oversize Packets/s**—Average number of data packets (excluding error packets) received per second that were more than 4352 octets in length, excluding framing bits but including FCS octets.

◆ **Beacons/s**—Average number of beacons observed per second; a node transmits these packets when it detects a hard failure upstream of itself.

◆ **Lost Frame Errors/s**—Average number of lost frame errors received per second on the network. Lost frame error indicates that the end delimiter of a frame is lost in the network. This counter represents the aggregate error of all types of frames including MAC and SMT.

◆ **Frame Copied Errors/s**—Average number of frame copied error frames reported per second by the station.

To configure a Segment Graph window, follow these steps:

Procedure 23
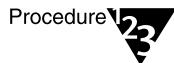
1. **With a Segment Graph window displayed and active, select** *Configure > Active Window***.**

   The Configure Segment Graph dialog box is displayed.

2. **If you want to use one of the supplied profiles, select one from the Profile box.**

   Profiles are available for Ethernet, token ring and FDDI segments.

3. **If you prefer to choose individual statistics instead of profiles, select the ones you want from the Statistic box.**

   You can select one statistic by clicking it, select several adjacent statistics by clicking and dragging, or select separated statistics by holding down the Ctrl key and clicking the ones you want. The following profiles are available: Destination, Errors, Default, and Utilization.

4. **If you want to save the new configuration as the default, click the Save as default check box at the bottom of the window.**

5. **Click OK.**

Examining Segments

ManageWise lets you display data for nodes on monitored token ring or FDDI segments. This data is useful to troubleshoot problems on the segment.

Examining Token Ring Stations

Information for nodes on a token ring segment is displayed in the Ring Stations window, shown in Figure 13-10.

Figure 13-10
Ring Stations Window

```
┌─────────────────────── #C9992251 - Ring Stations ──────────────── ▼ ▲
│ Order │ Node      │ State          Duration │ Soft Errors │ Beacons Upstream │
│     1 │ 2_0_TEST  │ On             0:28:27  │           0 │                0 │
│     2 │ CHARLES   │ On             0:28:28  │           0 │                0 │
│     3 │ KAREN     │ On  (Monitor)  0:28:28  │           0 │                0 │
│     4 │ NEIL      │ On             0:28:28  │           0 │                0 │
│     5 │ BOB_S     │ On             0:28:30  │           0 │                0 │
│     6 │ QA_2_B    │ On             0:28:30  │           0 │                0 │
│                                                                               │
│ ← │                                                                       │ → │
└───────────────────────────────────────────────────────────────────────────┘
```

The window title shows the segment name. The node names show ring order and indicate which is the Active Monitor. The columns show the

374   ManageWise 2.6 Network Management Guide

statistics, explained in Table 13-5, which are cumulative since NetWare LANalyzer Agent was started and are updated every 10 seconds.

Table 13-5
Ring Stations Window Statistics

Statistic	Explanation
Order	Relative position of nodes on the ring.
Node	Name of the node (or address, if the name is not in the ManageWise database).
State	Status of the node: ◆ *On.* The node is on the ring. ◆ *Off.* The node is off the ring. ◆ *On (Monitor).* The node is on the ring and is the Active Monitor.
Duration	How long this node has been On or Off.
Soft Errors	Number of soft errors in packets transmitted by this node.
Beacons Upstream	Number of beacon frames received by this node.
Beacons Downstream	Number of beacon frames transmitted by this node.
Duplicate Addresses	Total number of duplicate address errors reported, generated when this node detects other nodes using its own address.
Line Errors	Number of retransmitted line errors indicating a fault upstream.
Internal Errors	Number of internal errors this node has reported. Internal errors generally indicate recoverable failure of a network adapter board.
Burst Errors	Number of burst errors reported by the downstream neighbor. Burst errors indicate that a node detects the absence of transitions for the required time.
AC Errors	Number of times this node could not interpret the Address Recognized Indicator (ARI) and the Frame Copied Indicator (FCI) during the ring process.
Abort Delimiters	Number of times a node transmitted an abort sequence. Abort sequences are usually transmitted when a node detects an error in frames it is currently transmitting.
Lost Frame Errors	Number of times a node transmitted a frame but failed to receive it back in its entirety.

Ring Stations Window Statistics

Statistic	Explanation
Receive Congestions	Number of times the node detected a frame addressed to its specific address but could not copy it (generally due to insufficient buffers).
Frame Copied Errors	Number of times a node detected a frame addressed to its specific address with either or both the ARI and FCI bits set to 1. (Indicates that another node is using its address.)
Frequency Errors	Number of times a node's internal clock differed from the ring clock.
Token Errors	Number of token errors. These occur when the token gets corrupted or when the Active Monitor does not see a new frame transmitted in the required amount of time. Only the Active Monitor can report this error.
Last Enter Time	Date and time the node last entered the ring.
Last Exit Time	Date and time the node last exited the ring.
MAC Address	Physical (MAC) address of the node.

To sort the table entries, rearrange the columns, and export the data from this table, refer to *ManageWise 2.6 Setup Guide.*

Examining FDDI Ring Stations

Information for nodes on a FDDI ring segment is displayed in the FDDI Ring Stations window, shown in .

Figure 13-11
FDDI Ring Stations Window

Order	Node	State	Duration	Beacons Upstre	Beacons Downst	Upstream Neighbou	DownStream N
1	BLR-LANZ-TST6	On	0:09:52	0	0	BLR-LANZ-TST3	0020AFFBFBC
2	BLR-LANZ-TST3	On	17:23:56	0	0	0020AFFBFBCF	BLR-LANZ-TST
3	0020AFFBFBCF	On	17:23:47	0	0	BLR-LANZ-TST6	BLR-LANZ-TST

Table 13-6
FDDI Ring Stations Window Statistics

Statistic	Explanation
Order	Relative position of nodes on the ring.
Node	Name of the node (or address, if the name is not in the ManageWise database).
State	Status of the node: ◆ *On*. The node is on the ring. ◆ *Off.* The node is off the ring.
Duration	How long this node has been On or Off.
Beacons Upstream	Total number of beacon frames sent by this station and detected by the probe.
Beacons Downstream	Total number of beacon frames detected by the probe that name this station as its upstream neighbor.
UpStream Neighbour	MAC address of the node upstream to this station on the logical ring.
DownStream Neighbour	MAC address of the node downstream to this station on the logical ring.
InCRC Errors	Total number of line errors reported by this node.
OutCRC Errors	Total number of CRC errors reported by the nearest active downstream neighbor of this station and detected by the probe.
Lost Frame Errors	Total number of lost frame errors received on the network. Lost frame error indicates that the end delimiter of a frame is lost in the network.
Host Insertions	Number of times the probe detected this station inserting onto the ring.
Last Enter Time	Date and time the node last entered the ring.
Last Exit Time	Date and time the node last exited the ring.
MAC Address	Physical (MAC) address of the node.

To display the Stations window for token ring, or FDDI ring, follow these steps:

Procedure ▼▼ 1. **Select a token ring segment, or FDDI ring segment from the Network Segments window.**

   The line containing the segment is highlighted, and the action bar buttons for that segment selection become enabled.

2. **Click the Ring Stations button for token ring segments, or FDDI Stations button for FDDI segments.**

   Alternatively, you can select a token ring segment from the internetwork map, and then select *Performance > Token Ring*. Select a FDDI ring segment from the internetwork map, and then select *Performance > FDDI Stations.*

Configuring the Ring Stations Window

You can configure the Ring Stations window to show only the active nodes or to show all nodes on the segment, including those that have been active during the last week.

To configure a Ring Stations window, follow these steps:

Procedure ▼▼ 1. **With a Ring Stations window displayed and active, select *Configure > Active Window*.**

   The Configure Ring Stations dialog box is displayed.

Figure 13-12 shows the Configure Ring Stations dialog box for token ring segment.

Figure 13-12 **Configure Ring Stations**
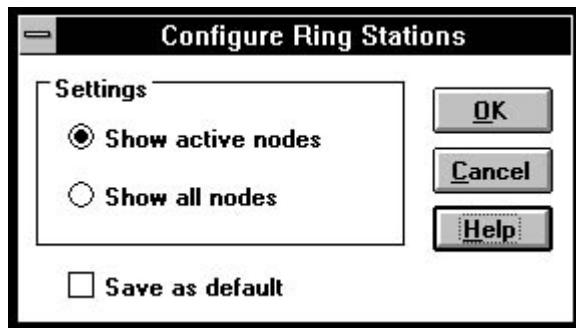
2. **In the Settings box, click the Show active nodes or Show all nodes option button.**

   ◆ Showing the active nodes displays those that are inserted into the ring and participating in the ring poll process.

   ◆ Showing all the nodes also displays nodes that are inactive but have been active during the past week. This can help you determine the order of the nodes on the segment.

Note ▼▼ Nodes that are inactive for more than a week no longer appear in the Ring Stations window. Also, a node that has been inactive since before NetWare LANalyzer Agent was installed is not recognized.

The default setting is to show active nodes.

3. **If you want to save the new configuration as the default, click the Save as default check box at the bottom of the window.**

4. **Click OK.**

Examining Segment Information

ManageWise provides the Segment Information dialog box to let you view and modify the segment information of the selected segment. Authorization for editing the information is controlled by the ManageWise Console password, if one has been set.

To display the Segment Information dialog box, follow these steps:

Procedure

1. Select a segment from the Network Segments window, the internetwork map, or a segment map.

The segment is highlighted.

2. Select _Edit > Database Object_.

The Database Object Editor window is displayed, with the Configuration Summary dialog box displayed.

3. Click the Segment Information icon.

The Segment Information dialog page, Figure 13-13, is displayed.

Figure 13-13
Segment Information Dialog Page
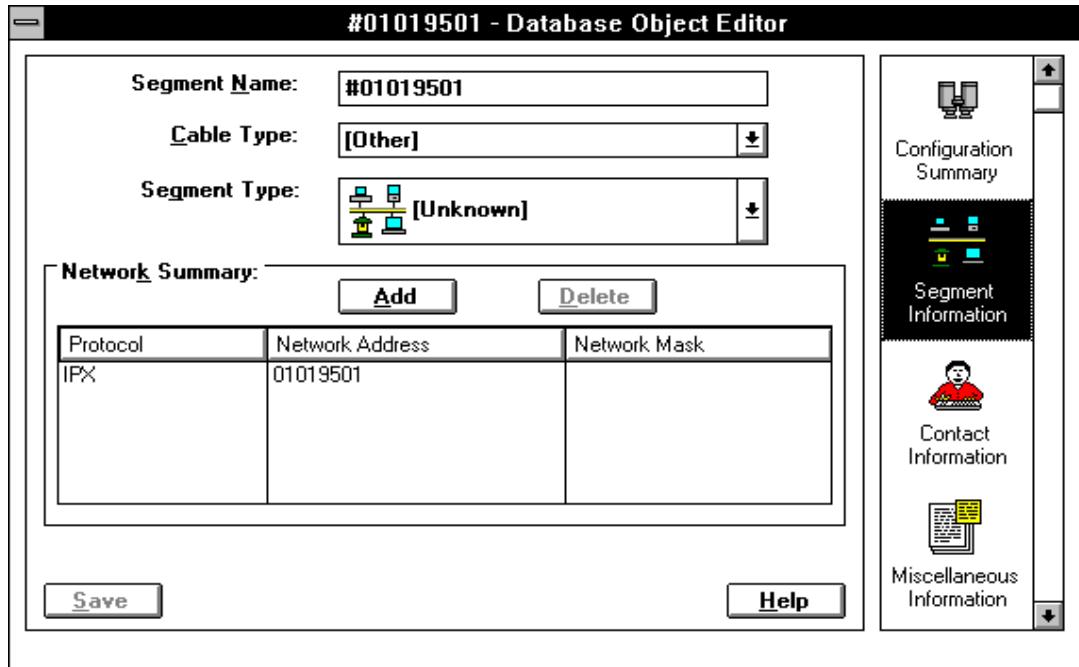
The dialog page gives more detailed information than the Configuration Summary window, including the segment name, cable type, segment type, protocols, and networks on the segment.

If no user-defined segment name is in the database, the segment name concatenates the names of the networks on the segment.

For more information about the Database Object Editor, refer to "Using the Database Object Editor" on page 50. For information about enabling and disabling segment alarms or choosing remote monitors, refer to "Enabling and Disabling Segment Alarms" on page 62 and "Choosing a Remote Monitor" on page 61, respectively.

Monitoring for Inactive Nodes on a Segment

For segments on which at least one NetWare LANalyzer Agent 1.1/1.2/ 1.21 (or LANtern network monitor with firmware 2.0) is installed, you can specify the nodes on the segment you want to monitor so that you are alerted if they become inactive. This Inactive Node Monitor feature has the following advantages:

◆ You can monitor any node on the segment, regardless of the protocol the node uses.

◆ You select the nodes on the segment that you want monitored. Monitoring continues even after you close the ManageWise Console. Therefore, when you reopen the ManageWise Console, you can see up-to-date information about which nodes are inactive.

◆ This feature does not impact network traffic because NetWare LANalyzer Agent does not poll the nodes to obtain their status.

Suggestion   Another way of monitoring connectivity is to define targets in the Connectivity Test window that you want ManageWise to ping periodically. However, unlike the Inactive Node Monitor feature described, the Ping Periodically feature polls the target nodes and generates traffic on the network. Also, the Ping Periodically feature is protocol-dependent. Therefore, we recommend that you use the Inactive Node Monitor feature instead of the Ping Periodically feature unless you need the statistics that the Connectivity Test window provides.

To specify nodes for which you want the status monitored, follow these steps:

Procedure   **1. Select one or more nodes.**

You can select one or more nodes from one of these windows: the segment's map window, the Ring Stations window, the (Top 20) Stations window, or the Conversations window.

2. Select *Fault > Inactive Node Monitor > Add.*

The nodes are added to the Inactive Node Monitor. The window also lists any nodes that were previously selected (in this session or a previous one).

Note ▼ You do not need to keep the Inactive Node Monitor window open or the ManageWise Console running for the nodes to be monitored because NetWare LANalyzer Agent is doing the monitoring, not the ManageWise Console. The ManageWise Alarm Manager must be running to record an inactive node in the Alarm Report. If the ManageWise Console is not running, check for alarms after you restart it.

You can open the Inactive Node Monitor window to check the Status column any time the ManageWise Console is running. To do this, follow these steps:

Procedure ▼ **1. Select a segment.**

You can select a segment from one of these windows: the segment's map window, the Ring Stations window, FDDI Stations window, the (Top 20) Stations window, or the Conversations window.

2. Select *Fault > Inactive Node Monitor > Status.*

To remove a node from the list of nodes whose status is monitored, follow these steps:

Procedure ▼ **1. Select one or more nodes.**

You can select one or more nodes from one of these windows: the segment's map window, the Ring Stations window, FDDI Ring Stations window, the (Top 20) Stations window, or the Conversations window.

2. Remove one or more nodes.

There are two procedures to do this. The first is to select *Fault > Inactive Node Monitor > Status* to open the Inactive Node Monitor window. Then, select the nodes you want to remove and click the Remove Nodes button, or select *Fault > Inactive Node Monitor > Remove.*

The second procedure is to open the segment's map, select the nodes you want to remove, and then select *Fault > Inactive Node Monitor > Remove.*

Capturing and Decoding Packets

ManageWise provides packet capture and decoding tools that help you analyze your network operations and identify the source of network problems.

Capturing and decoding packets can help you troubleshoot network problems by giving you detailed information about what is actually happening on the segment.

The following sections explain how you can use ManageWise to perform packet capture and decode operations:

◆ "Capturing Packets" on page 384

◆ "Displaying Captured Packets" on page 393

◆ "Viewing the Summary Window Pane" on page 395

◆ "Filtering Packets for Display" on page 403

◆ "Saving and Opening Packet Files" on page 408

Capturing Packets

One of the responsibilities of NetWare LANalyzer Agent on each segment is to capture packets on the segment. When the ManageWise Console sends a command to start capturing packets, NetWare LANalyzer Agent does so, and stores them in a buffer in memory. Then, as the ManageWise Console sends commands to display packets, NetWare LANalyzer Agent sends them to the ManageWise Console. Because only a small amount of data is sent at a time, the network is not overloaded. The methods ManageWise uses to display decoded packets minimize traffic on a network.

The ManageWise Console can request packet capture on several segments. Each NetWare LANalyzer Agent captures packets on the segment it monitors and stores them in its own local buffer.

If you prefer not to capture all packets that NetWare LANalyzer Agent sees, you can specify a *capture filter* that enables you to capture only selected packets. Similarly, after capturing packets, if you prefer not to display all the packets you captured, you can create a *display filter* to display only a defined group. You create these filters by choosing from among the following filter criteria:

◆ Only packets sent to, from, or between selected nodes

◆ Only packets of a specified protocol type

You can also control the slice size of the packet to make better use of the capture buffer.

To capture packets, follow two steps:

◆ Define a capture filter

◆ Start capturing packets

While capturing packets, you can also do the following:

◆ Stop packet capture

◆ Restart packet capture

◆ Create simultaneous packet captures

◆ Delete a capture buffer on NetWare LANalyzer Agent

These operations are explained in the following sections.

Defining a Capture Filter

ManageWise provides a capture filter with default values you can use to capture packets on any segment with NetWare LANalyzer Agent (you can choose the segment from the Network Segments window or from a map). You can also modify the values by performing the following steps:

◆ Specify the source and destination addresses as well as the direction; that is, packets only *to* a node, only *from* a node, or all packets *between* two nodes.

◆ Specify protocol types of packets to capture. ManageWise recognizes the following protocols:

- ◆ NetWare

- ◆ AppleTalk

- ◆ TCP/IP

- ◆ SNA

- ◆ DECnet

- ◆ NETBEUI

- ◆ XNS

- ◆ OSI

- ◆ Banyan* Vines*

◆ Specify a slice length. A slice specifies the maximum number of bytes of each packet, counting from the packet header, to keep in the buffer. This economizing helps you maximize the number of packets you can store in your buffer space, as well as reduce the load borne by NetWare LANalyzer Agent to process captured packets.

If you want to decode protocol header information, you need only 100 to 150 bytes. The rest is typically data that you need only if you suspect a data corruption problem. However, on certain very large packets, slicing can cause incorrect decodes by truncating information.

◆ Specify a capture buffer size and whether to stop packet capture when the buffer becomes full or to overwrite the oldest packets in the buffer with newer ones.

NetWare LANalyzer Agent attempts to provide the buffer size requested. If not enough space is available in server memory for a large buffer, ManageWise creates the size it can. You can see the final buffer size in the Capture Status window (refer to "Starting Packet Capture" on page 391).

◆ Specify what kind of packets to capture on Ethernet, token ring, or FDDI segments:

   ◆ **Ethernet**—Only good packets, only error packets, or both good and error packets.

   ◆ **Token ring**—All packets, non-MAC packets, or MAC packets.

   ◆ **FDDI**— All packets, LLC packets, MAC packets, or SMT packets.

For example, you might want to capture only NetWare packets sent by a certain node. You define a filter so you can capture only those packets that interest you. As a result, the buffer has more space to store your selected packets.

Note When you specify a capture filter, you are specifying the packets to capture (include) in the buffer on NetWare LANalyzer Agent, not the packets to exclude. When you specify both a node and a protocol, packets must meet both criteria to be captured. If you select more than one protocol family, packets can meet either protocol criterion to be captured.

To define a capture filter, follow these steps:

Procedure

1. **Select a segment.**

   You can select a segment by doing one of the following:

   ◆ Select *View > All > Network Segments* and select a segment

   ◆ Select a segment from the internetwork map

   ◆ Open a segment map

2. **Select *Performance > Capture Packets* or, if it exists, click the Packet Capture button in the action bar.**

   You can set up a filter for traffic with one or two nodes, rather than filtering on an entire segment. To do so, select one or two nodes from a map, the Stations table, or the Conversations table, and then select *Performance > Capture Packets*.

   The Packet Capture Setup dialog box is displayed. Figure 13-14 shows an Ethernet Packet Capture Setup dialog box.

Figure 13-14
Ethernet Packet Capture Setup Dialog Box
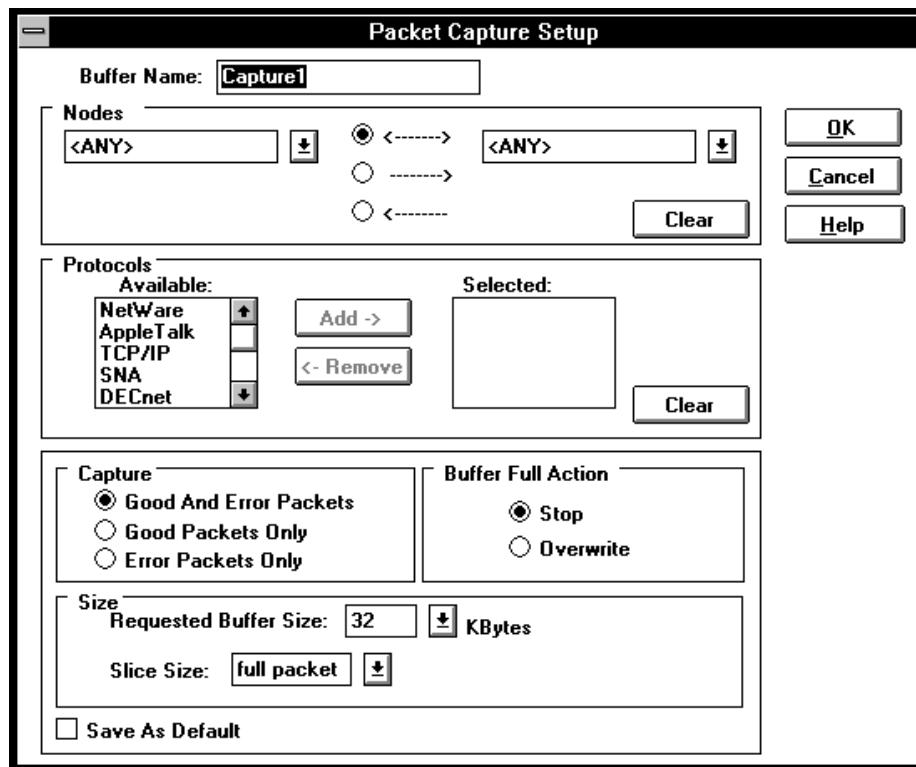
A token ring Packet Capture Setup dialog box looks identical, except for the Capture box, Figure 13-15.

Figure 13-15
Token Ring Capture Box
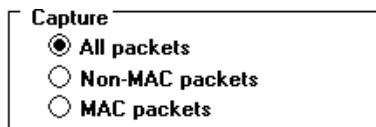
Figure 13-16 shows the Capture box for FDDI Packet Capture Setup dialog box.

Figure 13-16
FDDI Capture Box
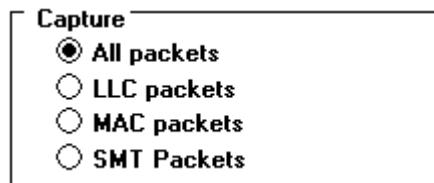
If you selected one node, it appears as the left node in the Nodes box; if you selected two, both appear in the Nodes box.

3. **If you want to name the buffer, enter a name in the Buffer Name text box or use the default name.**

   The buffer name helps you keep track if you are capturing packets on several networks at once. The name appears in the title of the Capture Status window and the Packet Display dialog box.

   ManageWise uses the default name Capture*n*, where *n* is the next available number in the sequence, starting with 1 each time you start ManageWise.

4. **If you did not select nodes from a map or table as explained in Step 1, you can type them in the Nodes text box or change either or both choices to ANY using the drop-down list box.**

5. **Select the direction of traffic flow between your nodes.**

   Click an arrow option button in the center of the Nodes box to select the direction of traffic flow. The available node and traffic flow directions are shown in Table 13-7.

Table 13-7
Traffic Flow Between Nodes

Node	Arrow	Node	Effect
node1	—>	node2	Capture packets that node1 sends to node2. This is equivalent to node2 <— node1.

Table 13-7 *continued*
Traffic Flow Between Nodes

node1	—>	ANY	Capture packets that node1 sends to any other node. This is equivalent to ANY <— node1.
node1	<—	node2	Capture packets that node2 sends to node1. This is equivalent to node2 —> node1.
node1	<—	ANY	Capture packets that any node sends to node1. This is equivalent to ANY —> node1.
node1	<—>	node2	Capture packets that node1 sends to node2 and packets that node2 sends to node1.
node1	<—>	ANY	Capture packets that node1 sends to any node and packets node1 receives from any node. This is equivalent to ANY <—> node1.
ANY	<—>	ANY	Capture all packets sent by or received from any node.

6. **If you want to filter on protocols used, add the ones you want to the Selected list box.**

   To add a protocol to the Selected list box, double-click it in the Available list box, or click it and then click the Add button. To delete a protocol from the Selected list box, double-click it, or click it and then click the Remove button. To empty the Selected list box, click the Clear button. You can select more than one protocol by clicking and dragging the mouse or by holding down the Ctrl key and clicking selected protocols.

   All protocols are selected by default when you first use ManageWise.

   Note   If no protocols are listed in the Selected list box, all protocols are captured.

7. **In the Capture box, select which packets to capture by clicking the appropriate option button for Ethernet, token ring, or FDDI segments.**

   ◆ **Ethernet**—Select whether to capture good packets, error packets, or both.

   ◆ **Token ring**—Select whether to capture MAC packets, non-MAC packets, or both (MAC packets are used to manage the operation of the token ring).

◆ **FDDI**— All packets, LLC packets, MAC packets, or SMT packets.

8. In the Buffer Full Action box, select what to do when the buffer is full by clicking the appropriate option button.

You can stop packet capture or continue packet capture and overwrite the oldest packets in the buffer.

Continuing packet capture means that no stop criteria exist and that new packets will overwrite ones already captured. You must stop packet capture manually from the Capture Status window.

9. In the Size box, select a buffer size.

Either select a buffer size from the drop-down list box or type in the size you want. The default buffer size is 32 KB.

10. In the Size box, select a slice size.

You can enter a specific slice length or select from the supplied slice lengths. Counting begins at the packet header.

Note Typically, less than 100 bytes are needed to fully decode the protocol information in a packet. By slicing packets, the protocol information from more packets can be captured in a particular buffer.

11. Click the Save As Default check box if you want to use the values you selected as the default values in the future.

Your capture filter is now set up. If you decide not to capture packets, click the Cancel button, in which case the dialog box closes and you return to the previous window.

Starting Packet Capture

You start capturing packets by clicking the OK button in the Packet Capture Setup dialog box.

The Packet Capture Setup dialog box closes and the Capture Status window, Figure 13-17, opens.

Figure 13-17
Capture Status
Window
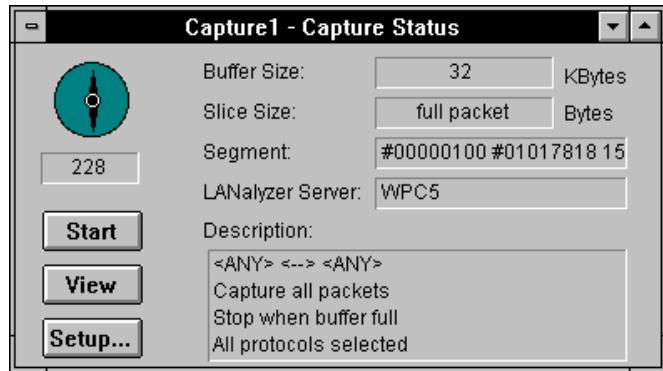
The capture buffer indicator needle begins to turn. As packets that meet your filter criteria are captured, a wedge on the dial turns green and a box below it displays the number of packets captured. When the dial is completely green, the capture buffer is full. If you choose to continue to capture packets when the buffer is full, new packets replace the oldest packets in the buffer.

Note The number of packets shown in the packet count can go down when the buffer is overwriting because one large packet can overwrite several small ones.

Stopping Packet Capture

When you set up your capture filter, you choose whether to stop packet capture when the capture buffer is full or to continue to capture packets but overwrite the oldest packets in the buffer. You must stop packet capture manually if you have not specified that the capture should stop when the buffer is full.

To stop packet capture manually, take one of the following steps:

◆ Click the Stop button in the Capture Status window. Packets stop being captured, and the Stop button label changes to Start. You can then restart the capture, close the window, or leave the window open and perform other functions.

◆ Click the View button in the Capture Status window. The Capture Buffer window is displayed and you can view decoded packets.

Note If you restart packet capture with the Packet Capture Setup dialog box, the existing packet capture stops.

Restarting a Stopped Packet Capture

When the Capture Status window is open, you can start and stop capturing packets using the Start/Stop button. If ManageWise is capturing packets, the button is labeled Stop; if it is not capturing packets, the button is labeled Start. The NetWare LANalyzer Agent buffer is cleared when you restart.

Creating Simultaneous Packet Captures

You can create simultaneous packet captures by repeating the procedure used to start the first capture. This enables you to set up and run captures with different capture criteria. You can start the next capture while an earlier Capture Status window is visible, or you can minimize the existing Capture Status window.

However, you can view only one capture buffer at a time. You must close an existing Packet Display window before opening another. Viewing capture buffers is explained in "Displaying Captured Packets."

Note ▼ Although you can view only one capture buffer at a time, you can save packet captures to a file and view as many files as you want, either while you are viewing a capture buffer or independently. Refer to "Saving and Opening Packet Files" on page 408.

Deleting a Capture Buffer

To delete a capture buffer, close the Capture Status window.

Note ▼ You can exit ManageWise while NetWare LANalyzer Agent is capturing packets. When you bring the ManageWise Console back up, the Capture Status window returns as an icon. NetWare LANalyzer Agent continues to capture packets according to the criteria you specified, even when ManageWise is not running.

Displaying Captured Packets

You can decode packets and view decoded packets in the capture buffer by clicking the View button in the Capture Status window (refer to Figure 13-17). The Packet Display window, Figure 13-18, is displayed. If you display this window while packets are being captured, capture automatically stops.

ManageWise retrieves packet data from NetWare LANalyzer Agent only as necessary for the ManageWise Console to decode and display the packets as you view them. This minimizes the amount of packet data transferred between NetWare LANalyzer Agent and ManageWise.

Note ▼ Although you can display multiple views of the same packet capture, as well as view multiple packet files, you cannot view more than one capture buffer at a time.

Figure 13-18
Packet Display Window
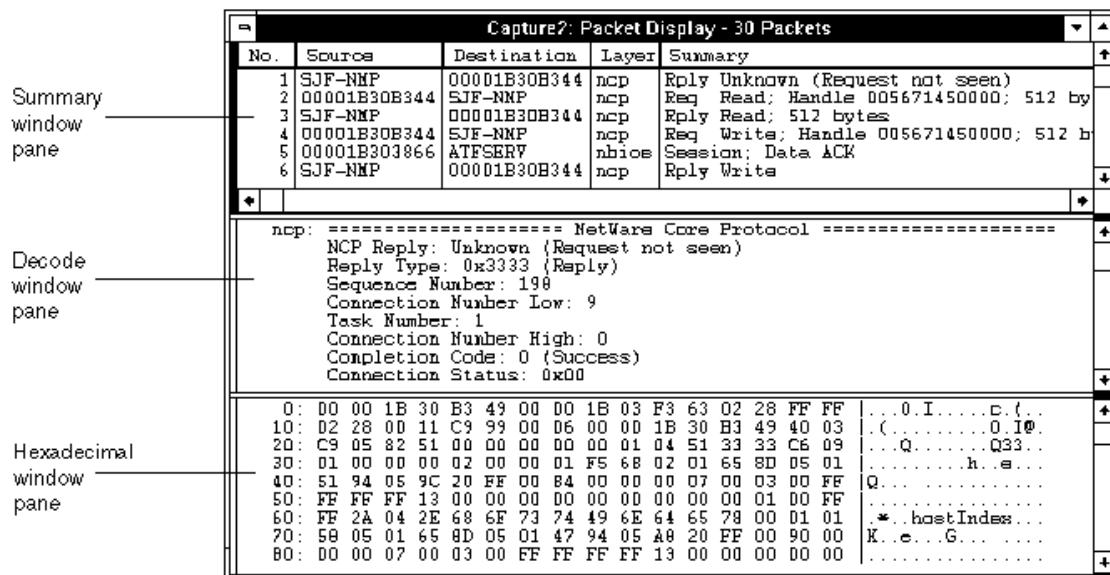
When you view captured packets, the Packet Display window contains three window panes that display captured and decoded packets:

◆ **Summary window pane**—Contains one-line summaries of each captured packet.

◆ **Decode window pane**—Displays one decoded packet in the format you select:

  ◆ Full decoding of each protocol layer and field (the default)

  ◆ One line per protocol layer

- **Hexadecimal window pane**—Displays the data in the selected packet in hexadecimal and ASCII or EBCDIC. If no ASCII or EBCDIC equivalent exists for a hexadecimal byte, a dot is displayed.

When you view packets initially, the first packet in the Summary window pane is highlighted and selected. The contents of that packet are displayed in the Decode window pane. The highest protocol layer in the packet is highlighted by default. If you select a different packet in the Summary window pane, it is highlighted and the Decode window pane displays its decoded contents.

Viewing the Summary Window Pane

The Summary window pane gives you an overview of the conversation between the source and the destination nodes. You select a packet in this window pane for further decoding and display in the other window panes. You can scroll the window pane horizontally, and you can change the size and position of the columns in the window pane.

The Summary window pane columns display the following information about captured packets:

- **No.**—Numbers the packets in order of arrival at NetWare LANalyzer Agent.

- **Source**—Name or the physical (MAC) address of the node that sent the packet.

Note Names are stored in the ManageWise database. If no name is found in the database, the MAC address is displayed. Refer to "Changing the Node or Segment Name" on page 57 for information about setting node names.

- **Destination**—Node to which the packet was sent. The node is displayed as the name or the physical (MAC) address of the node.

- **Layer**—Abbreviation of the highest protocol layer in the packet. It might display *ncp* for NetWare Core Protocol™ (NCP™) software, *ether* for the Ethernet Datalink layer, *rtmp* for the AppleTalk Routing Table Maintenance Protocol layer, or *802.2* for the IEEE 802.2 Logical Link Control layer. (If you choose the full decode option, the Decode window displays the full name of the protocol layer and all its fields. The Hexadecimal window pane shows the entire packet.)

◆ **Summary**—Brief description of the contents of the highest protocol layer.

◆ **Errors**—Type of errors, if any, in the packet.

◆ **Packet size**—Number of bytes in the packet. Packet size always excludes packet preamble and the cyclic redundancy check (CRC).

◆ **Interpacket time**—Time elapsed from the end of the preceding packet to the end of the current packet.

◆ **Absolute time—**Clock time on your PC when the packet arrived.

◆ **Relative time**—Time that elapsed since the arrival of the first packet still in the buffer.

Viewing Decoded Packets

ManageWise lets you display detailed information about the contents of a selected packet using the Decode window pane. The packet contents are interpreted (*decoded*) and displayed by protocol fields.

The Configure Packet Display dialog box provides the following choices for viewing a decoded packet:

◆ **Full decoding**—Provides information about each field in each protocol layer in a selected packet. This is the default decoding. Figure 13-20 and Figure 13-22 illustrate full decoding.

◆ **One-line decoding**—Provides a line of information for each protocol layer of a selected packet. Figure 13-21 illustrates one-line decoding.

◆ **Initial highlight position**—Places the initial highlighting at the highest protocol layer in a packet (the default) or at the packet header. The initial highlighting position is only a convenience. You can set it and change it as needed. Figure 13-20 and Figure 13-21 illustrate highlighting the highest protocol layer, and Figure 13-22 illustrates highlighting the packet header.

To set the decoding options, open the Packet Display window and follow these steps:

1. **Select *Configure > Active Window*.**

   The Configure Packet Display dialog box is displayed.

Figure 13-19
Configure Packet
Display Dialog Box
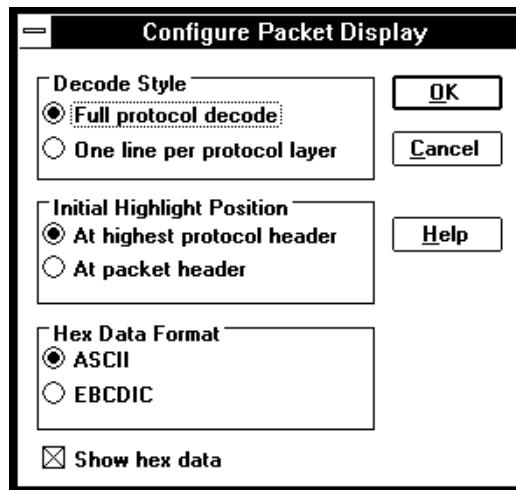
2. **Click the option button next to the decoding style you want.**

3. **Click the option button next to the initial highlight position you want.**

4. **Click the option button next to the type of format you want.**

5. **If you want to display the Hexadecimal window, select the check box labeled Show hex data.**

Figure 13-20
Decode Window Pane Showing Fully
Decoded Packet, Highlighting the Highest
Protocol Layer
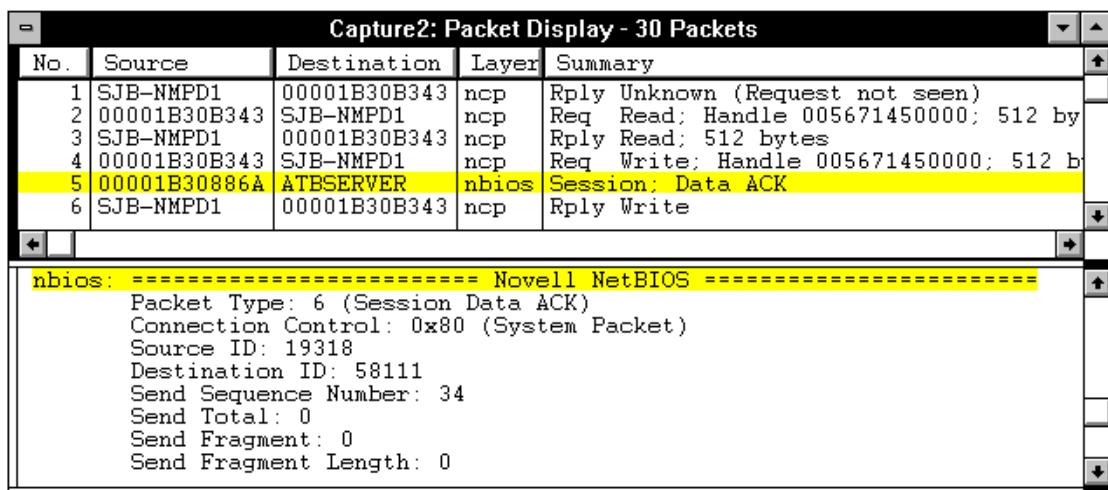
```
┌─────────────────────────────────────────────────────────────────────────┐
│ ▬        Capture2: Packet Display - 30 Packets              ▼ ▲          │
├───┬──────────┬────────────┬─────┬──────────────────────────────────────┤ ↑
│No.│ Source   │ Destination │Layer│ Summary                              │
├───┼──────────┼────────────┼─────┼──────────────────────────────────────┤
│  1│SJB–NMPD1 │00001B30B343│ncp  │Rply Unknown (Request not seen)       │
│  2│00001B30B343│SJB–NMPD1 │ncp  │Req  Read; Handle 005671450000; 512 by│
│  3│SJB–NMPD1 │00001B30B343│ncp  │Rply Read; 512 bytes                  │
│  4│00001B30B343│SJB–NMPD1 │ncp  │Req  Write; Handle 005671450000; 512 b│
│  5│00001B30886A│ATBSERVER │nbios│Session; Data ACK                     │
│  6│SJB–NMPD1 │00001B30B343│ncp  │Rply Write                            │ ↓
├───┴──────────┴────────────┴─────┴──────────────────────────────────────┤
│ ◄ █                                                              ►        │
├───────────────────────────────────────────────────────────────────────┤
│ nbios: ========================= Novell NetBIOS =====================    │ ↑
│        Packet Type: 6 (Session Data ACK)                                 │
│        Connection Control: 0x80 (System Packet)                          │
│        Source ID: 19318                                                  │
│        Destination ID: 58111                                             │
│        Send Sequence Number: 34                                          │
│        Send Total: 0                                                     │
│        Send Fragment: 0                                                  │
│        Send Fragment Length: 0                                           │ ↓
└───────────────────────────────────────────────────────────────────────┘
```

Figure 13-21
Decode Window Pane Showing One-Line
Decoded Packet, Highlighting the Highest
Protocol Layer

```
┌─────────────────────────────────────────────────────────────────────────┐
│ ▬        Capture2: Packet Display - 30 Packets              ▼ ▲          │
├───┬──────────┬────────────┬─────┬──────────────────────────────────────┤ ↑
│No.│ Source   │ Destination │Layer│ Summary                              │
├───┼──────────┼────────────┼─────┼──────────────────────────────────────┤
│  1│SJB–NMPD1 │00001B30B343│ncp  │Rply Unknown (Request not seen)       │
│  2│00001B30B343│SJB–NMPD1 │ncp  │Req  Read; Handle 005671450000; 512 by│
│  3│SJB–NMPD1 │00001B30B343│ncp  │Rply Read; 512 bytes                  │
│  4│00001B30B343│SJB–NMPD1 │ncp  │Req  Write; Handle 005671450000; 512 b│
│  5│00001B30336A│ATBSERVER │nbios│Session; Data ACK                     │
│  6│SJB–NMPD1 │00001B30B343│ncp  │Rply Write                            │ ↓
├───┴──────────┴────────────┴─────┴──────────────────────────────────────┤
│ ◄ █                                                              ►        │
├───────────────────────────────────────────────────────────────────────┤
│ 802.3: Protocol=NetWare; Length=48                                       │
│ ipx  : Type=IPX; Socket: NetBios–>NetBios                                │
│ nbios: Session; Data ACK                                                 │
│                                                                           │
│                                                                           │
└───────────────────────────────────────────────────────────────────────┘
```

398   ManageWise 2.6 Network Management Guide

Figure 13-22
Decode Window Pane Showing Fully
Decoded Packet, Highlighting the Packet
Header

```
┌──────────────────────────────────────────────────────────────────────┐
│ ▬              Capture2: Packet Display - 30 Packets          ▼ │ ▲ │
├─────┬────────────┬─────────────┬──────┬────────────────────────────┬───┤
│ No. │ Source     │ Destination │ Layer│ Summary                    │ ▲ │
├─────┼────────────┼─────────────┼──────┼────────────────────────────┼───┤
│   1 │ SJB-NMPD1  │ 00001B30B343│ ncp  │ Rply Unknown (Request not seen)│
│   2 │ 00001B30B343│ SJB-NMPD1  │ ncp  │ Req  Read; Handle 005671450000;512 by│
│   3 │ SJB-NMPD1  │ 00001B30B343│ ncp  │ Rply Read; 512 bytes       │   │
│   4 │ 00001B30B343│ SJB-NMPD1  │ ncp  │ Req  Write; Handle 005671450000;512 b│
│   5 │ 00001B30336A│ ATBSERVER  │ nbios│ Session; Data ACK          │   │
│   6 │ SJB-NMPD1  │ 00001B30B343│ ncp  │ Rply Write                 │ ▼ │
├─────┴────────────┴─────────────┴──────┴────────────────────────────┼───┤
│ ◄ │                                                               │ ► │
├────────────────────────────────────────────────────────────────────┼───┤
│ Packet Number : 5                    11:42:21PM                     │ ▲ │
│ Length : 66 bytes                                                   │   │
│ 802.3: =================== IEEE 802.3 Datalink Layer ================│   │
│         Station: 00-00-1B-30-38-6A ----> ATFSERVER                  │   │
│         Length: 48                                                  │   │
│   ipx: ================= Internetwork Packet Exchange ===============│   │
│         Checksum: 0xFFFF                                            │   │
│         Length: 48                                                  │   │
│         Hop Count:  0                                               │ ▼ │
└──────────────────────────────────────────────────────────────────────┘
```

Viewing the Hexadecimal Packet Data

The Hexadecimal window pane shows uninterpreted packet data in hexadecimal format. The ASCII or EBCDIC portion of the Hexadecimal window pane (to the right) displays a dot for every hexadecimal byte that has no ASCII or EBCDIC equivalent.

The first column in the window pane indicates the offset in hexadecimal bytes. The *offset* is the number of bytes counting from the beginning of the header. For example, the first three lines have the following offset:

◆ Hexadecimal 0: indicates zero offset

◆ Hexadecimal 10: indicates decimal 16 offset (16 bytes precede this)

◆ Hexadecimal 20: indicates decimal 32 offset (32 bytes precede this)

Whether you display one-line decoded or fully decoded packets in the Decode window pane, you can display entire packets in the Hexadecimal window pane. The Hexadecimal window pane and the highlighting tool (refer to "Highlighting Protocol Fields and Hexadecimal Bytes" on page 401) are especially helpful with the full-decode display when you are trying to associate protocol fields with specific bytes in a packet.

You can select *Configure > Active Window* (as explained in "Viewing Decoded Packets" on page 396) to display the Configure Packet Display dialog box and choose how to display the hexadecimal data. The Show hex data check box is selected by default. The Hex Data Format box enables you to select the format for the hexadecimal data. The hexadecimal data is shown in either ASCII or EBCDIC format. If you do not want to display hexadecimal decoded packet information, deselect the Show hex data check box.

Changing the Size of the Packet Display Window Panes

You can change the size of the Packet Display window panes by moving the divider between windows.

To change the size of a window pane, follow these steps:

Procedure

1. Place the tip of the mouse pointer in the space between window panes.

The pointer shape changes into a bar with arrows pointing up and down.

2. Press and hold down the left mouse button while you move the pointer up or down the screen.

3. Release the mouse button.

The window panes above and below the divider bar are resized to the new position of the divider bar.

Selecting and Decoding a Different Packet

You can select a different packet for decoding by following *one* of these steps:

◆ From the Summary window pane in the Packet Display window, scroll through the packet list and click a different packet. You can also use the arrow keys on your keyboard to move the highlighting to a different packet.

◆ Select *View > Go To Packet*. You are prompted for a packet number. After you enter the number, that packet is displayed and decoded in the Packet Display windows.

Note ▼ Packets are retrieved from NetWare LANalyzer Agent as you move the highlight through their headers in the Summary window pane using the mouse or the arrow keys. Using the `Go To Packet` command avoids transferring unneeded packet data from NetWare LANalyzer Agent. Similarly, scrolling the Summary window pane with the scroll bar retrieves only the packet header data when creating the decode summary, whereas using the arrow keys retrieves all packet data, needed or not.

Highlighting Protocol Fields and Hexadecimal Bytes

ManageWise provides a highlighting tool that can help you to associate protocol fields and hexadecimal bytes. Highlighting can be a useful training tool for new network managers who want to learn about protocol decoding.

You can use this tool in the following ways:

◆ You can highlight a protocol layer in the Decode window pane. This highlights all bytes in the selected protocol layer of the hexadecimal window pane.

◆ You can click a field in any of the protocol layers in the Decode window pane. This highlights the associated bytes in the Hexadecimal window pane.

◆ You can click hexadecimal bytes in the Hexadecimal window pane. This highlights all hexadecimal and ASCII or EBCDIC bytes of this field in the Hexadecimal window pane and the associated field in the Decode window pane.

◆ You can click ASCII or EBCDIC text in the Hexadecimal window pane. All hexadecimal and ASCII or EBCDIC bytes that belong to the field are highlighted in the Hexadecimal window pane, and the associated field is highlighted in the Decode window pane.

Figure 13-23 shows highlights in the Packet Display window that identify the selected packets in the Summary window pane, the associated fields in the Decode window pane, and the associated hexadecimal bytes and ASCII or EBCDIC data in the Hexadecimal window pane.

Figure 13-23
Highlights in the Packet Display Window
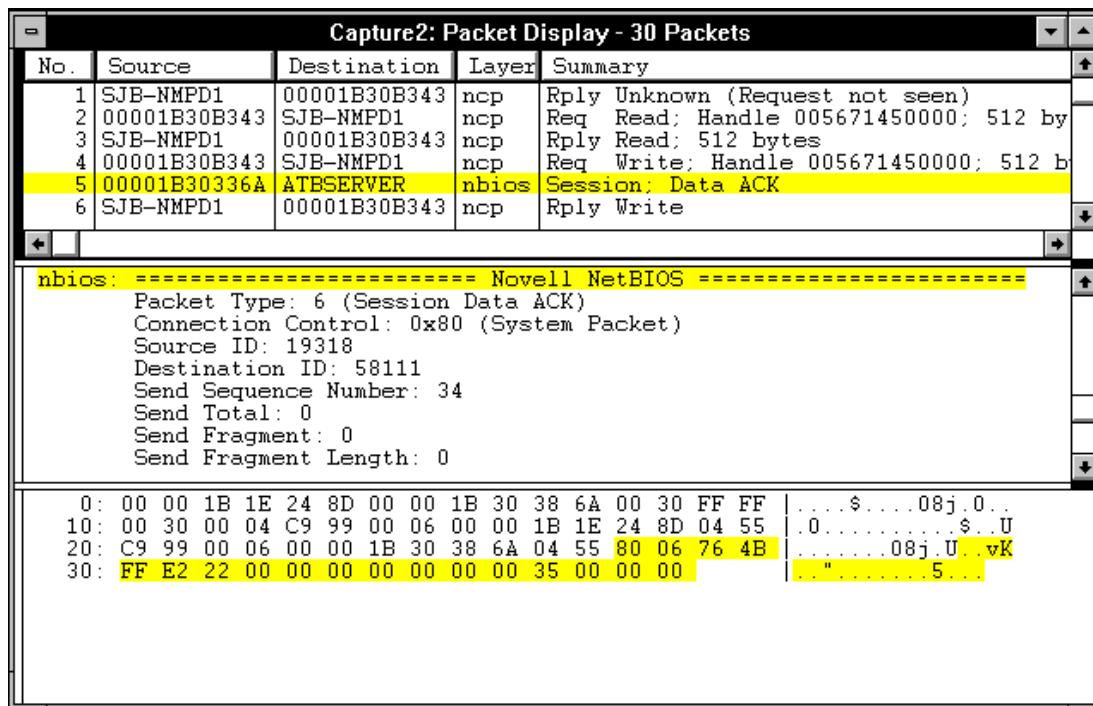
Filtering Packets for Display

After you have captured packets, you can apply a display filter to the capture buffer and view only the packets that interest you. You can filter on node names or addresses, protocol families or protocol layers, or contents of a selected field. This is useful if, for example, after you have captured packets, you realize you have a problem with a specific workstation and you want to display only packets it has sent or received.

Note ▼ Display filtering requires the transfer of a portion of every captured packet from NetWare LANalyzer Agent to the ManageWise Console. For large captures, this consumes time and network bandwidth. We recommend that you define very specific capture filters rather than filtering during display. However, subsequent filtering of the same capture results in no additional data transfer from NetWare LANalyzer Agent because the data is already transferred to the ManageWise Console. Therefore, it is much quicker to filter the same packet capture a second time.

Display filters affect only the display; they do not change the capture buffer. All captured packets remain in the capture buffer and are available for viewing with a different display filter or no display filter at all.

You can define a display filter in either of two ways:

◆ By selecting *View > Filter Packets*. The system provides a dialog box for defining the display filter.

◆ By using point-and-click filtering. You double-click a packet in the Summary window pane or a selected protocol layer or protocol field in the Decode window pane or in the Hexadecimal window pane. The system automatically sets up a filter based on the item you selected. You can also modify the filter information as needed.

Defining the Display Filter

To define a display filter, follow these steps:
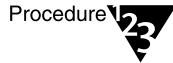
Procedure ▼ **1. Capture packets using the capture filter of your choice.**

2. View the packets.

3. Select *View > Filter Packets*.

The Display Filter dialog box, Figure 13-24, is displayed.

Figure 13-24
Display Filter Dialog Box
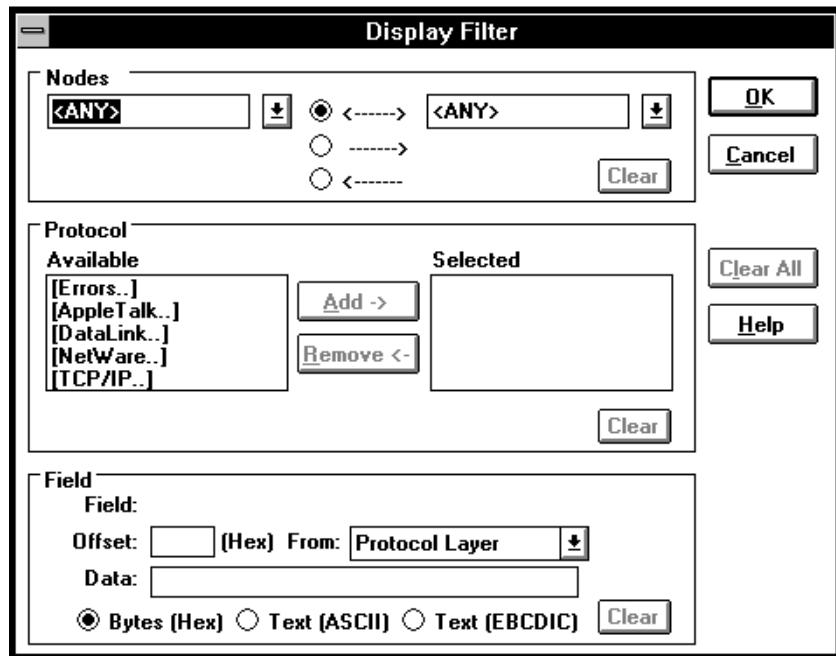
4. **If you want to filter on nodes, select the appropriate nodes and the direction of traffic flow between them.**

   4a. **Select the nodes from the two drop-down list boxes.**

   Alternatively, you can type a node name or address in place of ANY in either or both of the drop-down list boxes.

   4b. **Click an option button next to the arrow in the center of the Nodes box that defines the direction of traffic flow you want.**

5. **If you want to display all the packets of a protocol suite, add one or more protocols to the Selected list box.**

   To add the protocol suite to the Selected list box, select the protocol in the Available list box and then double-click it or click the Add button.

6. **If you want to display all the packets of a specific protocol layer, follow these steps:**

6a. **Double-click the protocol suite name in the Available list box to display a list box of all the protocols in the suite.**

Figure 13-25 illustrates a NetWare example.

Figure 13-25
Available List Box
NetWare Example
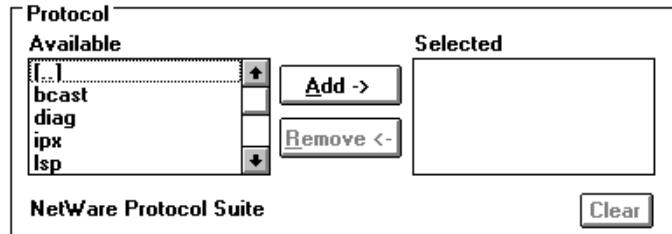
6b. **Scroll through the list to find the protocol you want.**

6c. **Double-click the protocol.**

7. **If you do not want to filter on a protocol that appears in the Selected list box, double-click it in the Selected list box to move it to the Available list box.**

8. **If you want to display all the packets that have the same contents in a specific field, follow these steps:**

8a. **Enter the offset *in hexadecimal bytes* in the Offset text box in the Field box.**

Figure 13-26 shows an example.

Figure 13-26
Offset Text Box
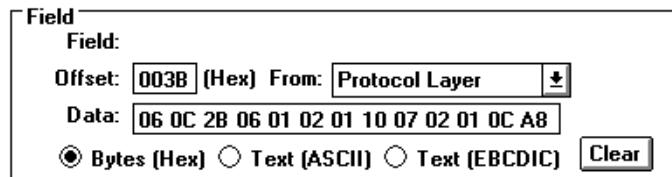
You can count the offset in the Hexadecimal window when the packet is decoded, using the offset column for guidance (refer to "Viewing the Hexadecimal Packet Data" on page 399 for more information).

8b. Specify whether the offset is counted from the beginning of the packet or from the beginning of a protocol layer.

Make your choice from the drop-down list box. If you choose the protocol layer option, you must select a specific protocol in the Protocol box.

8c. Click the appropriate option button to indicate whether you want to enter the data in hexadecimal, ASCII, or EBCDIC format.

8d. Enter the data in the Data text box that you want to include in the filter.

You can also fill in the values using point-and-click filtering, as explained in the following section, "Point-and-Click Filtering."

9. Click OK.

The dialog box closes and ManageWise begins to select the packets from the capture buffer.

If you have a large capture buffer, ManageWise displays the first packets that pass the filter. ManageWise continues to filter in the background while you examine these packets.

The Packet Display window title shows the number of packets available for display after the filter is applied. The Summary window shows the list of filtered packets that met the criteria in the display filter. You can view and decode them as described earlier in this section.

Point-and-Click Filtering

You can define a display filter using the point-and-click method by double-clicking a field in the Packet Display window.

When you double-click a highlighted field in the Packet Display window, the Display Filter dialog box is displayed. The following

procedure demonstrates the point-and-click filtering feature and illustrates the Display Filter dialog box.

To use the point-and-click method to define a display filter from the Packet Display window, follow these steps:

Procedure 23

1. **If you want to display only packets in one conversation (for example, between a node and a server), double-click a packet in that conversation in the Summary window pane.**

   (The Packet Display window is displayed when you click the View button on the Packet Status dialog box.)

   The Display Filter dialog box shows the source and destination of the selected packet. You can also modify the addresses, if needed. For example, you can change the destination address to ANY, to the broadcast address, or to a specific node address.

2. **If you want to display all the packets containing a specific protocol layer, double-click the protocol line in the Decode window pane.**

   The Display Filter dialog box shows the protocol you selected.

3. **If you want to display all packets with the same contents as a specific field, double-click the field in the Decode window pane or in the Hexadecimal window pane.**

   The Display Filter dialog box shows the field, the offset, the data, and the type of data for the selected field.

4. **Click OK.**

   The dialog box closes and ManageWise begins to select the packets from the capture buffer. The count of packets that match the filter is displayed in the window caption. The progress of the filter operation is displayed by the progress icon in the status bar.

   The Summary window pane displays the list of packets that met the display filter criteria. You can view and decode them as described earlier in this section.

Saving and Opening Packet Files

You can save captured packets to a file and open the file later for analysis or printing. You might want to save packets to a file in the following situations:

◆ To transfer the packets to another system or give them to someone else for analysis.

◆ To apply a display filter to decoded captured packets so you can view only the packets that interest you. After you apply the display filter, you can save the filtered packets to a file.

◆ To compare packets saved from your buffer with other packets. You can either save the other packets as well or view them from the capture buffer. You can view only one active capture buffer at a time. However, after you have saved packets to a file, you can open as many files as you want, and simultaneously view a capture buffer, if desired.

When you save packets to a file, ManageWise creates a binary file with the name you specify.

Note ▼ Packet files are compatible with LANalyzer for Windows and ManageWise. For example, packets captured and saved using LANalyzer for Windows can be viewed using ManageWise.

Saving Captured Packets to a File

To save captured packets to a file, follow these steps while viewing the capture buffer:

Procedure ▼ **1. If you do not want to save all the packets you captured, filter your packets first (refer to "Filtering Packets for Display" on page 403).**

When you save packets, you save only those that pass the display filter. If you did not filter the display, all packets are saved.

2. Select *File > Save As*.

The Save Filtered Packets or Save Unfiltered Packets dialog box is displayed, depending on whether you filtered your packets.

3. **Enter the desired name in the File Name text box. The file extension .TR1 is appended automatically.**

4. **Click OK.**

Opening Packet Files

To open a packet file, follow these steps:

Procedure

1. **Select *File > Open > Packet File*.**

   The Open dialog box is displayed.

2. **Double-click the name of the file you want to open.**

Printing Packets

To print packets, decoded or otherwise, follow these steps:

Procedure

1. **Open a Packet Display window, either by capturing packets or by opening a packet file.**

2. **Select *File > Print*.**

   The Print dialog box opens.

3. **Select the print options you want.**

   You can select the destination, format, and which packets to print:

   ◆ Choose whether to print to your default printer or to a file. If you choose a file, enter its name and specify whether the current packet data should overwrite the file or be appended to it.

   ◆ Choose whether you want a summary of the packet information, only the hexadecimal information, a full decode, or a brief decode. These formats correspond to the three window panes described in "Displaying Captured Packets" on page 393.

   ◆ Choose whether to print all packets, a range of packets, or only the filtered packets.

4. **Click OK.**

chapter **14** *Testing Connectivity*

ManageWise® software provides a test facility that enables you to verify that you have a good communication path from the ManageWise Console to devices in your internetwork.

This chapter describes how to use the ManageWise test facility. You can either test connectivity to a network device with which you suspect a problem or monitor one or more critical network devices, such as servers or routers, continuously. In the latter case, ManageWise generates an alarm if a target fails to respond. It enables you to detect problems proactively.

Testing Device Connectivity

If you suspect a problem with a network device such as a server or router, you can run the ManageWise connectivity test to determine whether your ManageWise Console can communicate with it.

The procedure you use to test connectivity varies, depending on whether you want to select the device on a map or specify the device name or address.

To test connectivity, follow these steps:

Procedure ▼ **23**

1. **Select the device on a map or go to Step 2.**

2. **Select *Fault > Ping Once*.**

The system displays the Connectivity Test dialog box.

```
┌─────────────────────────────────────────────────────────────┐
│ ▭                    Connectivity Test                         │
├─────────────────────────────────────────────────────────────┤
│ ┌─Category──────────────────────────────────┐   ┌─────────┐  │
│ │  ⦿ Name          │ SFF-TRITON          │   │ │  Test   │  │
│ │                                             │   └─────────┘  │
│ │  ○ IPX Address   │            │ : │       │  │ ┌─────────┐  │
│ │                                             │   │ Cancel  │  │
│ │  ○ IP Address    │   │·│   │·│   │·│   │   │   └─────────┘  │
│ └─────────────────────────────────────────────┘               │
│ ┌─Status──────────────────────────────────────┐               │
│ │ 'SFF-TRITON'  is alive.                       │  ┌─────────┐ │
│ │                                               │  │  Help   │ │
│ └─────────────────────────────────────────────┘  └─────────┘ │
└─────────────────────────────────────────────────────────────┘
```
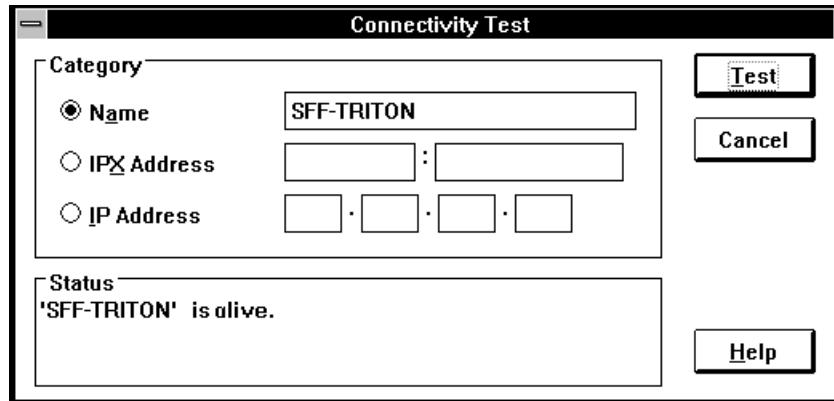
3. **If you have not selected a device on a map, select a Category option and type a corresponding device name or address.**

As a general rule, select the Name category if you do not know the address of the host to be tested. If the host supports both IP and IPX™ protocols, you can choose between them.

You must type a name exactly. If the name contains any wildcard characters and multiple objects match the name, the first object in the database is used.

Note   ManageWise truncates long names on maps. Therefore, the name of a device on a map might not be the exact name. To view the exact name of a device, select *Edit > Database Object* and view the Configuration Summary dialog page.

If an IPX or IP address is entered, that address is used for the connectivity test. If any of the edit boxes in the IPX address or the IP address are left blank, they are considered to contain zero. An IP address or an IPX address of all zeros is not valid. When an invalid address has been entered in the address boxes, the Test button is disabled.

4. **Click Test.**

If you selected Name, the name of the device is looked up in the database. If found, the IPX or IP address for that name is used and the appropriate connectivity test packet is sent. If the name is not

found in the database, ManageWise attempts to resolve the name to an IP address by means of the Domain Name System (DNS) or the local HOSTS file. If the name cannot be found, the connectivity test cannot continue.

If you selected IPX Address, an IPX connectivity packet is sent to the target device.

If you selected IP Address, an ICMP echo test packet is sent to the target device.

The system displays the response in the Status section of the dialog box.

5. Close the dialog box.

Monitoring Device Connectivity

If you want to monitor critical network devices continuously, such as servers or routers, you can define targets and perform periodic echo tests. For example, you might have critical servers that should always be active. Using this facility, you can monitor those servers continuously and receive alarms when they are not responsive.

Note You must keep the Connectivity Test window open the entire time you are monitoring.

Defining Targets

You can define targets for monitoring connectivity from the ManageWise Console to a network device in two ways:

◆ Select a target from an active ManageWise window that contains network devices. To do so, click the icon or table entry that represents the device.

For example, you can select target devices by clicking icons from the internetwork map, segment map, or custom map. Or, you can select target devices from windows that display a table of device entries, such as View All Servers ("Monitoring File Servers" on page 164), Routers summary ("Displaying Global Routers Summary" on page 238), system entries in IPX Networks, IPX Node List, IP Node List, or Address Details windows. (See Chapter 15, "Managing Network Addresses.")

To make multiple selections in a window, hold down the Ctrl key while selecting.

◆ Define a target explicitly in the Add Target dialog box. This dialog box is displayed when you select *Fault > Ping Periodically* without selecting a target from an active ManageWise window (as described in the preceding bullet). This method lets you specify targets that are not necessarily in the ManageWise database. Refer to the online help for a description of how to define targets using the Add Target dialog box.

Invoking the Test Facility

If you selected a network device from an active ManageWise window, select *Fault > Ping Periodically* to start the test. The system displays the Connectivity Test table, as shown in Figure 14-1. The default test interval is 5 seconds.

If you did not select a network device from an active ManageWise window, selecting *Fault > Ping Periodically* displays the Add Target dialog box. After you specify targets in the Add Target dialog box, the system displays the Connectivity Test table, shown in Figure 14-1. Refer to the online help for a description of the Add Target dialog box.

Figure 14-1
Connectivity Test Table

The Connectivity Test table lists all defined targets and displays the test results. The tests stop running when you close the window. The Save and Load commands let you create and use various test profiles.

Table 14-1 explains the columns in the Connectivity Test table.

Table 14-1
Connectivity Test Table Columns

Column	Explanation
Target	Name of the network device for which the communication path is being tested. If you do not specify a name in the Add Target dialog box, this field is blank.

Table 14-1 *continued*
Connectivity Test Table Columns

Column	Explanation
Status	General test status of the target. It displays one of the following values: 1. `OK`. Communication path between the ManageWise Console and the target is OK. 2. `Response timeout`. Indicates one of the following scenarios: ◆ Defined target is not operational. In this scenario, ManageWise uses the Test Connectivity facility as a node monitor on your internetwork. ◆ ManageWise Console and the defined target are not in the same network and the router failed to route the test packets. To confirm this scenario, run *Fault > Test Connectivity > Once* to the routers in the path. 3. `Target unreachable`. ManageWise does not know how to send a packet to the target. That is, none of the routers adjacent to the ManageWise Console can forward packets to the target. This can happen if a NetWare® server is down or if any of the intermediate routers between the ManageWise Console and the target is down.
Sent	Number of echo test messages sent from the ManageWise Console to the target.
Received	Number of echo test responses received by the ManageWise Console from the target.
Last Received	Time the last echo test message was received by the ManageWise Console from the target.
Round Trip Delay	Moving average round trip time for an echo message to be sent from and received by the ManageWise Console. Currently, this value is displayed for IP targets only.
Enabled	Specifies whether the test is enabled.
Interval	Interval, in seconds, at which the echo test is performed. Different test intervals can be specified for different targets. The default test interval is 5 seconds.
Retries	Number of retries for a response before an alarm is generated.
Protocol Address	Protocol address for the selected target. If you select a target from an active ManageWise window, the protocol used for echo test depends on that application. IP is the default protocol if a target supports multiple protocols.

Specifying Number of Retries before Generating Alarms

The ManageWise test facility generates an alarm when it receives no response from a device after a specified number of retries. To specify the number of retries in either the Add Target dialog box or the Test Interval dialog box, refer to the online help.

For detailed information about alarms, refer to Chapter 6, "Understanding Alarms."

chapter **15** *Managing Network Addresses*

The ManageWise® internetwork and segment maps described in Chapter 2, "Using Maps," provide a graphical representation of your network. This chapter describes windows within the ManageWise Console that list the network numbers and addresses for the entities displayed in the internetwork and segment maps. You can use this information as an aid when you assign and maintain network numbers and addresses.

IPX Network Numbers

An IPX™ network number is a 4-byte hexadecimal value used in routing IPX packets in the internetwork. To view all IPX network numbers in your internetwork, select *View > All > IPX Networks* from the main menu bar. ManageWise generates an IPX Networks table, as shown in Figure 15-1.

Figure 15-1
IPX Networks Table

The IPX Networks table lists all external and internal IPX network numbers in use during network discovery. Each network number, internal or external, must be unique across the internetwork.

The top of the IPX Networks table displays an action bar. The action bar buttons function as follows:

◆ **Refresh**—Updates the table with current database information.

◆ **Summary**—Summarizes network information. Displays the total count of physical and internal networks discovered in the database.

◆ **Help**—Displays online help. This is equivalent to pressing the F1 key.

Table 15-1 explains the fields in the IPX Networks table.

Table 15-1
IPX Networks Table Fields

Field	Explanation
Network Number	Eight-digit hexadecimal number that uniquely identifies a network.
Media Type	In the case of an external network number, this field contains the media type of network, such as *Ethernet*. If the discovery process has not figured out the media type, this field might contain the value *Unknown*.
	For internal network numbers identifying a NetWare® server system, this field contains the value *Internal network*. This value might be displayed in gray if all details of a system are not fully resolved by the discovery process.
	This field might also contain the value *NetWare IP*. In this case, the 8-digit network number identifies a logical group of NetWare/IP™ nodes on which the NetWare services are implemented on top of TCP/IP instead of IPX.
System Name	Name of the system, in case of an internal network number. The field is blank if the value in the Media Type field suggests an external network number or NetWare/IP domain.
Duplicates	Each network number must be unique in the internetwork. However, if a duplicate number is assigned and the discovery module happens to be active, the information is recorded in the ManageWise database and reported in this field.

You can also display the addressing details of any network in the IPX Networks table. To do so, double-click the network entry. The system begins to read the database. It then displays one of the following tables:

◆ Address Details Table

◆ IPX Nodes Table

◆ NWIP Nodes Table

Address Details Table

If the entry selected in the IPX Networks table is an internal network number used by a NetWare server system, ManageWise displays the Address Details table, shown in Figure 15-2. This table lists all IPX and IP network addresses that the selected system is known by. Each instance represents a protocol binding to an adapter card and the corresponding network address used by the bound protocol. Figure 15-2 shows a system with two adapter cards, each bound with an IP and IPX address.

Figure 15-2
Address Details Table

Table 15-2 explains the fields in the Address Details table.

Table 15-2
Address Details Table Fields

Field	Explanation
Network Address	Network address of the system. If the entry selected is displayed in gray (that is, discovery is still in progress), this field contains the value *Unknown*.
Protocol	Protocol for the corresponding network address field.
Frame Type	Method used to encapsulate a network-layer packet over a media. For example, Ethernet II and Ethernet 802.3 are possible types over an Ethernet media. If the entry selected is displayed in gray, this field contains the value *Unknown*.
MAC Address	MAC address of the network interface board to which the corresponding network address is bound.

IPX Nodes Table

If the entry selected in the IPX Networks table is an external network number, ManageWise displays the IPX Nodes table, shown in Figure 15-3. This list displays all IPX nodes discovered on the selected network. It can be viewed as a tabular display of the corresponding segment map with IPX nodes only.

Figure 15-3
IPX Nodes Table

130.57.248.0 Subnet - IP Nodes

IP Address	System Name	MAC Address
13.57.248.1	Legal Beginning Address	00-00-00-00-00-00
13.57.248.252	SNF-PRD-CISCO.NOVELL.COM	00-00-0C-01-C4-3F
13.57.248.253	SNF-DEV-CISCO.NOVELL.COM	00-00-0C-02-0B-04
13.57.248.254	SNF-WAN-CISCO.NOVELL.COM	00-00-0C-02-0A-FB
13.57.251.254	Legal Ending Address	00-00-00-00-00-00

Table 15-3 explains the fields in the IPX Nodes table.

Table 15-3
IPX Nodes Table Fields

Field	Explanation
IPX Address	Ten-byte value used in addressing an IPX node. If the node is a NetWare 3™ server or router, the IPX address consists of the 4-byte internal network number assigned to the system, followed typically by 000000000001. If the node is a NetWare 2 server or workstation, the IPX address consists of the 4-byte external network number that the node is connected to, followed by the 6-byte MAC address.
System Name	Name assigned to a NetWare server or router. For a workstation, this field is likely to contain a 12-digit text string representing the MAC address.
Service Types	Types of service the node has (according to the discovery process). Examples are NetWare Server or IPX Router.

NWIP Nodes Table

To view all the NetWare/IP nodes belonging to a selected domain (as recorded in the ManageWise database), double-click an entry in the IPX Networks window for which the media type column lists NetWare/IP. The NWIP Nodes table appears, shown in Figure 15-4.

Figure 15-4
NWIP Nodes Table
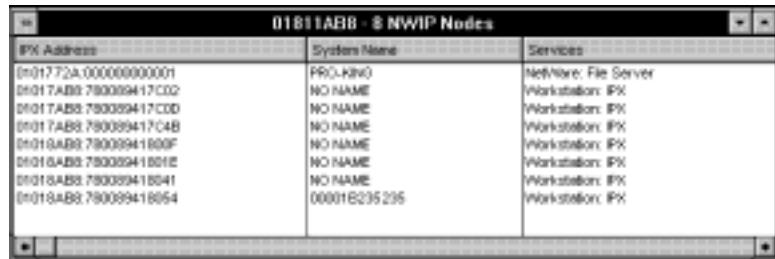
Table 15-4 explains the fields in the NWIP Nodes table.

Field	Explanation
IPX Address	IPX address of that node.
System Name	Name of the system.
Services	Services on this node.

IP Network Numbers

To view all IP network numbers in your internetwork, select *View > All > IP Networks.* ManageWise generates the IP Networks table, shown in Figure 15-5.

The IP Networks table lists all IP network numbers in logical order. Subnet masks are listed as well. The table makes you aware of the partitioning of your IP internetwork.

The action bar buttons at the top of the table work exactly like those in the IPX Networks table. Refer to "IPX Network Numbers" on page 419 for a description of the action bar and the buttons.

Table 15-5 explains the fields in the IP Networks table.

Table 15-5
IP Networks Table Fields

Field	Explanation
Network Number	Network address in four-part dotted decimal notation.
Subnet Mask	Subnet mask in dotted hexadecimal notation.
Media Type	Media type of the network, such as Ethernet.
Subnet Mask	Subnet mask in dotted decimal notation.

You can also display a list of all IP nodes on any IP network in the database. To do so, double-click an entry in the IP Network window. The system begins to read the database. It then displays the IP Nodes table, shown in Figure 15-6.

Figure 15-6
IP Nodes Table

Table 15-6 explains the fields in the IP Nodes table.

Note ▼ ManageWise calculates the range of legal IP addresses for each pair of network number and subnet mask. The first and last entries in the IP Node List describe this range and are displayed in light gray to distinguish them from the discovered addresses. You can use these values in assigning IP addresses.

Table 15-6
IP Nodes Table Fields

Field	Explanation
IP Address	IP address of the system in four-part dotted notation.
System Name	Name of the system.
MAC Address	MAC address of the network interface board to which the corresponding IP address is bound.

p a r t

VI *ManageWise Management Strategies*

ManageWise® software provides many powerful tools you can use to monitor and manage your network. Chapter 16, "Using ManageWise to Maintain Network Performance," presents strategies you can use to make the best use of ManageWise and keep your networks in optimum working order.

ManageWise Management Strategies

chapter **16** *Using ManageWise to Maintain Network Performance*

The following sections introduce three kinds of strategies you can use to maintain the performance of your network using ManageWise® software:

◆ "Creating a Network Baseline"

This section explains how to collect and record network statistics so you can track the performance of your network over time, anticipate problems, and justify new equipment or upgrades.

◆ "Solving Network Problems Using ManageWise" on page 436

This section explains how to use ManageWise to solve several common network-related problems.

◆ "Management Tips" on page 437

This section suggests several ways to use ManageWise to help you manage your network.

Creating a Network Baseline

To track network growth and performance, you need to create a performance baseline for each critical device as a benchmark against which you can measure changes. Then you create new baselines for each device at regular intervals or when you add a new server, workstation, router, or application. Reviewing the performance of the devices or segments over a period of time enables you to set them up for optimum performance and plan for growth. In addition, you can spot chronic problems and justify upgrades and expansion.

One way you can maintain network performance is to take the following four steps:

◆ Create a baseline

The time to create your baseline is during normal conditions on a network that is in good working order. Doing so gives you a representative picture of how your network should operate. After tracking a characteristic, you can set thresholds for 20 to 30 percent over that number so you are alerted when the characteristic rises, possibly indicating network growth.

When you record characteristics, it is best to sample over several days to a week, rather than for a short interval such as a day: the short interval might be atypical and might not provide a representative sample.

◆ Record the baseline

To track changes in your network, you need to keep a record of each device and segment so you have data you can refer to at need. Doing so enables you to compare current numbers with those from, for example, six months ago. Spotting trends helps ensure that you can avoid problems by solving them before they arrive.

To keep a record of the performance of each device and segment in your network, you can print the tables and graphs by selecting *File > Print* and keep them in notebooks for each segment (refer to *ManageWise 2.6 Setup Guide* for an explanation of printing from ManageWise).

Note If the scale makes the graphs hard to understand, you can change it before printing.

You might also want to export data for use by a spreadsheet program. You can create a data file and append information each time you record a baseline. This enables you to keep the data online. To export data, select *File > Export*, as explained in *ManageWise 2.6 Setup Guide*.

◆ Set alarm thresholds

As you work with your network and develop a sense for its typical operation, you can set thresholds based on its typical levels. For example, if you examine your trend graph for a segment and discover that your utilization peaks at around 27%, you can choose to set your alarm threshold at 35%.

ManageWise enables you to set alarm thresholds and choose the sampling interval for a variety of errors. Refer to Chapter 6, "Understanding Alarms," for more information.

◆ Interpret the alarms

When an event triggers an alarm, you need to know what it indicates about your network and what to do about it. If you select an alarm in the Alarm Report window or the Alarm Disposition table, and then click the NetWare® Expert™ button, a help window appears that explains the alarm and suggests how to resolve problems.

Although you can choose to baseline any critical object in your network, certain types of objects are almost universally useful. The following sections explain how to baseline servers and segments. You can choose to baseline additional kinds of objects, depending on your network.

Creating Server Baselines

You can create baselines for servers that have NetWare Management Agent™ software installed and that have been discovered by NetExplorer™ software and, therefore, show up in maps. The server icon shows red and yellow file folders on the map, showing that NetWare Management Agent is installed; plain white folders indicate it is not installed.

Note ▼ ManageWise trending can create these baselines automatically. You can save a year's worth of data, or more, for any parameter monitored by ManageWise.

When you double-click the server icon, the server Configuration window opens. This window gives you access to the characteristics you want to baseline.

The characteristics listed in the following sections are vital to track. As you work with your network, you might find other characteristics to watch, but these characteristics are primary. For a detailed explanation of NetWare server parameters, refer to *Utilities Reference* in your NetWare server documentation.

Server Memory Utilization

On a NetWare server, virtually all processes are handled through server cache. Therefore, having sufficient cache buffers is one of the key characteristics of server performance.

To view cache information, double-click the RAM icon in the server Configuration window for the server you are monitoring. (For more information, refer to "Monitoring Memory Usage" on page 172.)

Click the Legend button to the right of the window to see what the colors on the pie chart stand for. Note the percentage given for cache buffers. If you are currently experiencing no problems with server performance, select *File > Export* to export the data to a file. If you are experiencing performance problems, try increasing the amount of memory; a safe amount is 65% to 70%, but this number can vary by network.

File Reads and Writes

This statistic lets you track the performance of the disk I/O channel and possibly identify bottlenecks. You can see file reads and writes by following one of these procedures:

◆ Open the All File Servers window and select a server. Click the Trends action bar button. Select *File System Reads* (both #/min and KB/min) and *File System Writes* (again, both #/min and KB/min). Click OK.

◆ Open the server Configuration window. Select the Open Files icon and click the Trends action bar button.

The Open Files—Trends graph is displayed. If you want, you can click the time bar at the bottom to place the cursor at a certain point; then click the Legend button to see the numeric values at that time. Select *File > Print* to print the graph.

CPU Utilization

Server CPU utilization typically rises when users and application NLM™ files are added to your server. Most, but not all, NLM files are written to relinquish control of the CPU if another process requires it. Therefore, where a server could typically sustain a utilization percentage of 75% with little degradation, you should record your

utilization over a period of time and look at the spikes. If typical usage is between 40% and 60%, you might set a threshold at 70%, then track how often alarms arrive. If the frequency of the alarms increases, you can begin to predict when performance will suffer and you need more CPU.

To see a graph tracking CPU utilization for a server, open the server Configuration window, double-click the CPU icon, and then click the Graph button. We recommend that you record CPU utilization over a 24-hour period and possibly over more than one day a week; usage patterns and backups might give you different data on different days.

You might find it useful to select *File > Export* to store the data in a file, then import it into a word processor. This enables you to enter comments about the data and any changes in the configuration since the last baseline. Over time, a series of such baselines lets you see when a significant change occurs.

Volume Utilization

Tracking volume utilization is more useful for planning for growth and capacity than for troubleshooting. As you track the volume space used over time, you can accurately predict when to purchase additional disk storage. Also, the documentation is useful when planning your budget.

Starting from the server Configuration window, you can display the Trends graph to track volume utilization using any of the following methods:

◆ To see all the volumes on a server, select the Volumes icon, then click the Trends action bar button. The Trends graph is displayed.

◆ You can also see utilization for only one volume:

   ◆ Double-click the Volumes icon, select your volume, then click the Trends action bar button. The Trends graph is displayed.

   ◆ With nothing selected, click the Trends action bar button and scroll to Free Space on Volume. Available volumes are listed in the Device column. Select the desired line. The Trends graph is displayed.

Select *File > Export* to export this data to a spreadsheet to compare changes over time.

NLM Files Loaded

Tracking loaded NLM files is especially important if you have multiple servers because you probably want the configuration of your servers to match. Three characteristics are important to track relative to NLM files:

◆ Which NLM files are loaded

◆ What version of each NLM is loaded

◆ How much memory each NLM is using

To view NLM information, open the server Configuration window and double-click the NLM files icon. The NLM Files table is displayed. You can now sort the columns by double-clicking the column heading. To list the NLM files alphabetically, sort the Name column. To sort the NLM files by amount of memory used, double-click the Memory column.

You can now select *File > Export* to export this sorted information to a spreadsheet. It is useful to keep a series of baselines in the same file so you can compare the data over time.

Baselining Segments

ManageWise provides a Trends graph you can use to record how any segment has been performing for the past hour and for the past 24 hours. You can display the graph for a selected segment by opening the Network Segments window (*View > All > Network Segments*) and selecting *Performance > Segment Trends*. Select *Configure > Active Window* to format it to display any statistic you choose.

The characteristics listed in the following sections are vital to track. As you work with your network, you might find other characteristics to watch, but these characteristics are primary.

Utilization Percentage

It is important to record utilization to track two factors:

◆ **Growth**—Tracks what happens to your network over time. As your network segments grow, utilization also grows. New workstations and applications place a heavier load on the network and cause performance to suffer.

◆ **Usage patterns**—Tracks how your network is used and when the peaks occur. Such information is useful for discovering what times of day the performance slows or for planning when to do backups.

Keeping track of these two kinds of utilization can also help you document the need for further growth and to plan the growth as the time approaches.

Utilization is based on kilobytes per second and packets per second and is compared with the maximum bandwidth possible. For Ethernet networks, the maximum possible is 10 Mbps; for token ring networks, the maximum possible is 4 or 16 Mbps (depending on the hardware). For FDDI networks, the maximum possible is 100 Mbps.

Error Rates

Tracking error rates helps you diagnose the performance of a network as it grows. A typical network will have a low level of errors, and knowing the typical levels for different kinds of errors enables you to tell when a problem is developing.

For example, as your utilization percentage grows, your error rate is also likely to grow. However, if your error rate grows faster than utilization, it signals a problem with a component in the network.

Kilobytes per Second

The number of kilobytes per second indicates the actual throughput of your network.

Packets per Second

The packets per second rate gives you a general idea of the amount of traffic on a wire. Because packets differ in size, this characteristic does not show utilization, which is based on the number of kilobytes. Utilization can increase as a result of either an increase in the number of packets or the size of packets.

Packets are sent as requests, replies, and information. If the number of packets increases but utilization does not, it indicates that the number of small packets has increased.

Solving Network Problems Using ManageWise

ManageWise provides many powerful monitoring tools that give you information about your network. You can set thresholds so that ManageWise alarms bring problems to your attention. You can also learn about conditions on your network by opening windows on devices and segments. Then, based on the information you receive, you can correct the problem, identify potential future problems, or store the information for later comparison or to document purchasing needs.

This section walks you through several common network problems and explains how you can use ManageWise to solve them.

User Cannot Log In/Attach to the Network

A user calls up, unable to attach to the network. Follow these steps to track down the problem:

1. Check whether the user has loaded the network driver. To do so, use ManageWise to perform a connectivity test. Find and select the user's workstation on a segment map, and then select *Fault > Ping Once.*

2. Look for reasons the user cannot communicate with the server. Check that the server is operating correctly.

3. If the server is operating correctly, set up a packet capture, ask the user to attempt to log in, and capture packets during the login process. You might discover an incompatible frame type or that the server is not responding because of insufficient connections.

4. Compare elements of the user's setup with those of a user who can log in. Check their configuration files, login scripts, and permissions.

Server CPU Utilization Is High

An alarm has just been generated that you have exceeded the CPU utilization threshold on a server. You now need to determine what caused the utilization to be that high. Follow these steps to track down the problem:

1. Check whether there are sufficient cache buffers to handle the requests coming in to the server. To do so, double-click the Memory icon in the server Configuration window.

   You can change cache buffers using the SET Parameters action bar button. If the cache buffers are less than 50 percent, try increasing memory before you consider putting in a faster CPU. If cache buffers are 65 percent or higher, they are not the cause of the problem. For an explanation of SET parameters, refer to the *Utilities Reference* in your NetWare server documentation.

2. If the cache buffers are 5 percent or higher, look at what NLM files are utilizing the CPU. To list what NLM files are running, click the NLM Files icon in the server Configuration window.

Management Tips

This section suggests additional ways you can use ManageWise to make network management easier.

Poll Critical Devices

Select *Fault > Ping Periodically* to set up a connectivity test to critical nodes. This ensures that if the nodes go down, you are informed immediately. You can also use the ManageWise capability of launching programs to, for example, a third-party paging program when the node goes down.

Create a Map of Only the Devices You Manage

Using ManageWise, you can create custom maps containing only objects you select. You can use this capability to create a map containing only objects you manage. This makes it easier for you to monitor those devices because you don't need to pick them out of a larger map. For

example, when an alarm is received on this map, you know it's yours. Refer to "Creating Custom Maps" on page 41 for more information.

Hub-Specific Information

For useful information about managing hubs, refer to "Tips and Techniques" on page 305.

appendix **A** *Using Remote Console*

ManageWise® software lets you access the NetWare® RCONSOLE utility to log in to a selected server and perform supervisory functions remotely. This enables you to manage your servers from your ManageWise Console rather than having to work at the server itself.

Note ▼ REMOTE.NLM and RSPX.NLM must be loaded on any server you access using Remote Console.

You can use Remote Console to change, load, and unload modules; execute console commands; and copy files to the server NetWare directories or DOS partition. You can also use Remote Console to change all the server values that ManageWise monitors.

For more information about RCONSOLE, refer to *Utilities Reference* in your NetWare server documentation.

Starting Remote Console

You can start Remote Console from the All File Servers window, from a server's Configuration window, or from the *Tools* menu. The procedure for starting Remote Console from either window is the same.

To open a remote console session, follow these steps:
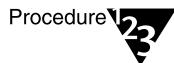
Procedure ▼ **1. Click the Remote Console action bar button.**

Alternatively, select *Tools > Remote Console*.

The Servers list box is displayed. Servers that you can remotely log in to are listed.

Note ▼ The list of servers in the Servers list box might not show all the servers to which you can attach. The Servers list box shows all of the servers in the server's bindery list to which your workstation is attached. Therefore, it is possible that on one workstation the Servers list box shows one list of servers, and on another workstation the Servers list box shows a different list of servers because it is attached to a different server.

2. **From the Servers list box, select a server.**

   If the server you want to access is not in the list, follow these steps:

   2a. **Click IPX Addr.**

   The Remote Console by IPX Address dialog box is displayed.

   2b. **Enter the IPX™ address of the server.**

   2c. **Enter the Remote Console password for the server.**

   2d. **Click OK.**

   The Remote Console session opens. Skip Step 3 and Step 4.

3. **Enter the Remote Console password.**

4. **Click OK.**

The Remote Console session opens.

G*lossary*

Acknowledge alarms

An action taken to indicate you have seen an alarm. Acknowledged alarms appear with a check mark on the alarm report. When all alarms logged against a station are acknowledged, the alarm indicator on the map (the bell icon) disappears.

Adapter

Hardware, typically an interface card, installed in a computer, that connects the computer to other hardware or devices.

Address

Identifier assigned to networks, stations, and other devices so that each device can be separately designated to receive and reply to messages.

Advertising

Process by which services on a network inform other devices on the network of their existence. NetWare uses the Service Advertising Protocol (SAP) to do this.

Agent

A piece of software on a networked system that prepares and accumulates information and communicates on behalf of a software entity. ManageWise supplies the following agents: NetWare Management Agent, NetWare LANalyzer Agent, and NetWare Hub Services. Third-party agent software can also be written for ManageWise.

Alarm

A notification of a network event or condition such as a server overload or a router that is not responding. Some alarms occur automatically for a particular device. Others are based on configuration of thresholds. *See also* **Alarm threshold**.

Alarm delta

The amount by which performance must fall below or rise above the alarm threshold before crossing the threshold again can trigger an alarm. Setting an alarm delta prevents repeated alarms when values fluctuate near a threshold.

Alarm disposition

The actions taken by ManageWise when an alarm of a certain type is received, such as logging the alarm in the database or calling your beeper. You set alarm dispositions by selecting *Fault > Alarm Disposition*.

Alarm family

A grouping of alarm types. For example, SNMP alarms are an alarm family.

Alarm Manager

The ManageWise component that receives alarms from the data acquisition modules, applies the appropriate alarm disposition, and passes the alarms to the Alarm Monitor and Alarm Report for display.

Alarm Monitor

The ManageWise component that provides a real-time display of all alarms, whether or not they are logged in the database.

Alarm Report

The ManageWise component that displays all alarms that have been logged to the database (as specified by the alarm disposition). New alarms are added to the display as they are written to the database. The Alarm Report also enables you to delete and acknowledge alarms, add comments to alarms, and display only alarms for selected devices.

Alarm threshold

A preset value that, when met or exceeded, triggers an alarm. *See also* **Alarm delta**.

Alignment error

An Ethernet error indicating that a packet was received that subsequently could not be framed properly. Therefore, the contents of the packet could not be interpreted properly and were rejected. These malformed packets might be the result of collisions, noise, or hardware failures. *See also* **Ethernet**, **Frame**.

Anchor

The object displayed in the upper-left corner of an ManageWise map. All network interconnection is shown as starting from that object. ManageWise lets you change the anchor using a button on the action bar.

Application Programming Interface (API)

A specification of input and results that can be used to develop software that accesses the capabilities of another application (such as ManageWise).

Autopartition

A mechanism by which a hub isolates a malfunctioning station or segment of the network from other, properly functioning, segments of the network. A station or segment is partitioned automatically if it is the source of a large number of consecutive collisions or is the source of abnormally long collisions. The segment remains partitioned as long as the condition persists.

Baseline

A snapshot of your network providing an example of network state, and including such factors as bandwidth usage and error rates. A series of baselines can be taken periodically and used to track network changes.

Block

A set of continuous bits or bytes that make up a definable quantity of information, such as a message.

Bridge

A device that connects two or more physical networks, forwarding frames between networks based on information in the data-link header. Because it operates at the data-link layer, it is transparent to the Network-layer protocols.

Broadcast

(noun) Packet delivery service in which all hosts on a network receive a copy of any frame that is designated for broadcast. (verb) Sending the message to all nodes.

Broadcast packet

A packet sent to all devices on a segment.

Btrieve

The database record manager used by ManageWise.

Buffer

Memory area or electronic register where data is stored temporarily while awaiting disposition. It compensates for differences in data-flow rates (for example, between a terminal and its transmission line). Also used as a data backup mechanism, holding data that might be retransmitted if an error is detected during transmission.

Byte

A group of eight consecutive binary digits (bits) operated on as a unit. All frames consist of an integer number of bytes. *See also* **Frame**.

Cache

A high-speed memory section that holds blocks of data that the CPU is currently working on; designed to minimize the time the CPU spends accessing memory.

Capture filter

A mechanism that enables you to define specific types of packets to capture, rather than capturing all packets. NetWare LANalyzer Agent captures only the specified types of packets on the segment where it resides. *Compare* **Display filter**.

Checksum

Numerical computation that combines the bits of a transmitted message; also, the resulting value. The value is transmitted with the message; the receiver recalculates the checksum and compares it to the received value to detect transmission errors. *See also* **CRC (Cyclic Redundancy Check) errors**.

Circuit

Any path that can carry an electrical current.

Client

A node or workstation on a network that requires services from a server.

Client-server model

A type of configuration that uses distributed intelligence to treat both the server and the individual workstations as intelligent, programmable devices.

Collision

An event (which is normal on any Ethernet network) that occurs when two or more nodes attempt to transmit simultaneously. Subsequent retransmissions are generally successful due to special algorithms implemented in every network controller that minimize the chance of consecutive collisions occurring.

A large number of collisions usually indicates a high load on the network but can also be caused by a network adapter board failure.

Connectivity test

A verification of the connection between the ManageWise Console and a target station, using either an IPX echo packet or an ICMP echo test packet.

Contention

A process that occurs when processors want to use the same communications lines. Each processor must send a request to transmit; if the channel is busy, the processor must wait.

CRC (Cyclic Redundancy Check) errors

An error-checking procedure using a predefined mathematical divisor to check the integrity of a transmitted block.

Custom map

A graphical representation that you can create with ManageWise to show a personalized view of your network. For example, a custom map can be created showing where all the company's sites are located and, for each site, a floor plan.

Database

A set of logically connected files that have a common access. All data entities that exist for several related systems. A database can have several data items that can be assembled into many different record types.

Data rate mismatch

An Ethernet error that indicates a significant difference in frequency between the clocks in the sending and receiving stations. A port reporting a data rate mismatch is usually connected to a faulty station.

If all (or a number of) ports report a data rate mismatch, the hub network controller contains a faulty clock source.

Discovery

The process of identifying internetwork topology and devices and storing the information in the ManageWise database, which the ManageWise Console uses to create maps. Discovery is done by the **NetExplorer system**.

Display filter

A mechanism that enables you to define a subset of the packets that have been placed in the buffer by NetWare LANalyzer Agent that you want ManageWise to display, rather than displaying all captured packets. *See also* **Capture filter**.

Distributed processing

A technique that enables multiple computers to cooperate in the completion of tasks, typically in a networked environment.

Domain

In the Internet, a part of a naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names separated by periods. In OSI, it is generally used as an administrative partition of a complex distributed system.

Encapsulation

A technique used by Network-layer protocols in which a layer adds header information to the protocol data unit from the preceding layer. Also used in enveloping one protocol inside another for transmission (for example, IP inside IPX).

Error detection

The process of determining whether one or more bits have changed from a one to a zero, or the reverse, during transmission.

Ethernet

A type of LAN that uses a bus topology and that accesses the media using Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Event

A network message that indicates operational irregularities in the physical elements of a network, or a response to the occurrence of a significant task.

FCS

See **Frame Check Sequence (FCS)**.

FDDI

See **Fiber Distributed Data Interface (FDDI)**.

Fiber Distributed Data Interface (FDDI)

ANSI standard for high-speed (100Mbps) fiber-optic connections.

File server

Shared storage device for LAN users, typically in the form of a personal computer that has a high-volume disk and is attached to the network. *See also* **Server**.

Filter

A mechanism that can be used to instruct NetWare LANalyzer Agent to capture only specific types of packets (a capture filter) or to limit ManageWise to display only a subset of the packets captured (a display filter). For example, you can capture or display only packets coming from a certain address. *See* **Capture filter** and **Display filter**.

Fragment

An Ethernet packet that contains fewer than 64 bytes and has a faulty Frame Check Sequence (FCS). A fragment is typically the result of a collision.

Frame

A packet data format for a given media. Some media support multiple packet formats (frames) such as Ethernet 802.2, Ethernet 802.3, Ethernet II, Ethernet SNAP, Token-Ring, or Token-Ring SNAP.

Frame Check Sequence (FCS)

A sequence of bits appended to Ethernet packets used to verify the integrity of a packet.

Frame Check Sequence (FCS) error

An error that occurs when a packet is involved in a collision, when it has been corrupted by noise, or when an error in the sending network controller occurs.

Frames too long

A condition that occurs when frames are longer than 1518 bytes, the maximum length of a well-formed Ethernet frame.

Gauge

A graphic display of the values of selected variables. Bar graph gauges show the current value, the high value, the maximum possible value, and the alarm-trigger value of the variable. You can change the alarm-trigger value.

Graph

A graphic display of trends or changes in data over time.

Graph scaling

A feature of the ManageWise graphs that enables you to scale the graph values so they are displayed in a certain range.

Hardware address

An address that is preprogrammed on a network interface card. *See* **Physical address**.

Header

The information at the beginning of a packet that defines control information, including addressing and control.

Historic data

The information about the prior state of a network, segment, or device, often stored in a file.

Hot fix area

A portion of the server hard disk to which NetWare redirects faulty data blocks. NetWare uses this method to ensure that data is stored safely.

Hub

A collection of one or more hub cards (also known as groups) that logically forms a single multiport repeater.

Hub card

A collection of ports in a hub, typically a PC adapter board that supports a number of 10BASE-T connections. (The terms *hub card* and *group* are sometimes used interchangeably, but the ManageWise product and manuals use the term *card*.)

Hub Management Interface (HMI) specification

A definition, developed by Novell, of how hub management functions are integrated into the Open Data-Link Interface (ODI) model. The HMI specification enables drivers to manage hubs resident in or external to a server.

INETCFG

A NetWare Loadable Module (NLM) that simplifies the installation of Novell internetworking products by enabling a network administrator to configure boards and enable parameters from a menu.

Internet

A collection of networks and gateways that use the TCP/IP suite of protocols. Lowercase, it is sometimes used as an abbreviation for internetwork.

Internet address

A 32-bit address assigned to hosts using TCP/IP.

Internetwork map

A logical rather than physical representation of your internetwork that shows segments and the routers that connect them. *See also* **Logical network map**, **Custom map**.

IP (Internet Protocol)

An industry-standard networking protocol, enabling dissimilar nodes in a heterogenous environment to communicate with one another.

IPX (Internetwork Packet eXchange)

A NetWare protocol, similar to the Xerox Network Systems (XNS) protocol, that provides datagram delivery of messages.

Jabber

A fault condition resulting from a network adapter that is stuck "on" and is transmitting packets continuously.

LAN

See **Local Area Network (LAN)**.

Late event

An Ethernet collision that occurs later in the transmission than should be possible, if the basic networking rules (protocols) are followed. Because stations listen for traffic before transmitting, collisions should occur only when two or more stations transmit nearly simultaneously, resulting in a collision early in the transmission.

A late collision indicates a faulty network controller or a violation of the rules of topology: network too big, too many repeaters connected in a series, and so forth.

Link state

An indicator of the health status of a 10BASE-T twisted-pair link. If a link is disconnected, turned off, or broken, the link state indicates "link down."

Load balancing

A scheme for distributing network traffic among parallel paths, providing redundancy while efficiently using the available bandwidth.

Load sharing

The ability of two or more remote bridges to share their traffic load in a parallel configuration; if one bridge fails, traffic is routed to the next parallel bridge.

Local Area Network (LAN)

A group of computers and other devices that are connected by a communications link that enables any device to interact with any other device on the network.

Logical network map

A graphical representation of your network resources that might not correspond to the physical location of the resources but, rather, shows connectivity. The ManageWise internetwork map is a logical network map because it shows how network segments are interconnected but does not show where those segments are physically located. *See also* **Internetwork map**, **Segment map**.

MAU

In IBM token ring networks, a multistation access unit. In IEEE 802.3 networks, a media attachment unit, which performs the physical layer functions of the Open Systems Interconnection (OSI) model.

Managed object

A device that is connected to a network and that can be managed by network management software or a protocol such as SNMP.

Managed server

Any server running the NetWare Management Agent software (a set of NLM files), which enables it to be monitored and managed remotely from the ManageWise software. The NetWare Management Agent software provides dynamic performance data about managed servers to the ManageWise Console.

ManageWise

The system of Novell and third-party applications that share the platform graphic user interface, database, and operating environment to discover, monitor, and manage devices on an Ethernet, token ring, or FDDI network running IP or IPX protocols. The system of applications can monitor and manage NetWare servers, hubs, routers, workstations, and segment-level operations.

ManageWise Console

The component of ManageWise used by a network administrator to interact with the network. The ManageWise Console software includes the ManageWise graphic user interface, database, alarm subsystem, and NetExplorer Manager. The ManageWise Console communicates with agents over the LAN using SNMP. It collects data on the behavior of the devices on the network. You then use the ManageWise Console to display, review, or acknowledge the data.

ManageWise database

A set of Btrieve files in which the ManageWise Console stores data about the discovered network topology, physical location of nodes, configuration, alarm notification, and alarm disposition.

ManageWise Server

A NetWare server running, at a minimum, NetWare Management Agent and MWISE.NLM. A ManageWise Server can also run NetWare LANalyzer Agent, the Desktop Management Tools, Virus Protect software, NetWare Hub Services software, and NetExplorer software. A ManageWise Server running NetExplorer software is referred to as a *NetExplorer Server. See also* **Managed server**.

MIB (Management Information Base)

A hierarchical database that stores management information for a network entity, such as a router, file server, or segment.

MIB Browser

An ManageWise facility that provides SNMP access to any MIB over IP or IPX, giving you the ability to retrieve data from any SNMP device or to set values on any SNMP device.

MIB Compiler

The software that compiles the concise MIB files into a binary file that is used by the MIB Browser.

MJLP (MAU jabber lockup protection)

A type of protection against jabber lockup in a transceiver or multistation access unit (MAU), which is an error state caused by an excessively long transmission repeated by a connected repeater. This feature is provided in Ethernet transceivers to prevent a jabbering adapter from disabling use of the network. Because it might be difficult to reset a MAU that is attached to or embedded in a repeater, repeaters disable the transmission of a jabbering port to prevent the attached MAU from entering jabber lockup. *See also* **Jabber**.

Multicast

A special form of broadcast in which copies of the packet are delivered to multiple stations, but only a subset of all possible destinations. *See* **Broadcast**.

Multiport repeater

See **Repeater**.

Name resolution

The ability to associate a name that the network administrator has assigned with its network location.

Name server

A server on the network that maps network names to network locations.

Navigator

An ManageWise feature that helps you move through a large internetwork map to pinpoint your specific areas of interest.

NetBIOS

Network Basic Input/Output System. Application program interface that is typically used on LANs comprising IBM and compatible microcomputers. Separates application programs from the networking subsystem, so that application program implementers can support multiple network designs, and a network system can support independently developed applications.

NETXPLOR.DAT

The sequential record file in which discovery data is stored temporarily on the NetExplorer Server. This file is usually open and should be excluded from server backups. Whenever NETXPLOR.NLM is unloaded, it writes over the existing file when it is loaded again. By default, ManageWise does not back up the file, but you can enable backups by specifying the value of a parameter in the NETXPLOR.NCF file on the NetExplorer Server.

NetExplorer

A term often used to refer indiscriminately to all the network discovery components that reside on a ManageWise Server, such as NETXPLOR.NLM, and the ManageWise Console, such as NetExplorer Manager software. *See also* **NetExplorer system**, **NetExplorer Manager.**

NetExplorer Manager

The component of the ManageWise NetExplorer system that resides on the ManageWise Console. NetExplorer Manager controls the timing and duration of updates from NetExplorer components on the NetExplorer Server. NetExplorer Manager also keeps track of the records that were sent previously, and directs NETXPLOR.NLM to start with a specified record number. This enables multiple ManageWise Consoles to receive data from the NetExplorer Server as needed.

NetExplorer system

The complete ManageWise network discovery software that has components on a ManageWise Server (NETXPLOR.NLM, NXPIPX.NLM, NXPIP.NLM, and NXPLANZ.NLM), and on the ManageWise Console (NetExplorer Manager). (A ManageWise Server running the network discovery software is referred to as the *NetExplorer Server.*) The NetExplorer Server components NXPIPX.NLM, NXPIP.NLM, and NXPLANZ.NLM discover segments, networks, and devices, and provide data to NETXPLOR.NLM. At the request of NetExplorer Manager, NETXPLOR.NLM sends data about new or changed objects to NetExplorer Manager.

NetWare

Novell's network operating system, which provides the ability to transparently share services across dissimilar platforms. Uses the NetWare Core Protocol (NCP), Internetwork Packet Exchange (IPX), and Sequenced Packet Exchange (SPX) protocols.

NetWare Expert

The online help component of ManageWise that focuses on three areas: tutorial, reference, and alarms. The tutorial guides you through interactive training on the ManageWise software; the reference is an online hypertext glossary of terms; the alarm help gives you help for individual alarms in the Alarm Report window.

NetWare Hub Services software

A group of NLM files that provides real-time information about NetWare 3.11 or later servers with HMI-compliant hub cards. It shows the number of hubs in each server, the number of cards in each hub, the number of ports on each card, the status and traffic volume for each port, and summary information for all ports, and gives you the ability to disconnect ports from the net.

NetWare LANalyzer Agent

The Novell SNMP-based remote monitor software that includes NLM files installed on NetWare 3.x, NetWare 4.x, or later servers. NetWare LANalyzer Agent discovers devices, gathers statistics, detects events and, on request, captures packets on segments on which it is installed. This remote monitor and the LANtern network monitor provide equivalent functionality; both can be monitored from ManageWise.

NetWare Link Services Protocol (NLSP)

The IPX link state protocol used by IPX routers to share information about their routes with other devices on the network. Enables network managers to interconnect small or large networks without routing inefficiencies.

NetWare Loadable Module (NLM)

A program you can load and unload from server memory while the server is running. The NetWare server allocates a portion of memory to the NLM when the NLM is loaded. The NLM uses the memory to perform a task, and then returns control of the memory to the operating system when the NLM is unloaded.

NetWare Management Agent

A set of NLM files installed in a NetWare server that enables the server to be monitored and managed remotely using SNMP. Servers running NetWare Management Agent are known as *managed servers*. NetWare Management Agent provides dynamic information about the server, such as CPU usage, NLM files loaded, and so on.

Network

In ManageWise, a component of a networking environment that corresponds to an IPX network address, an IP network address or, if applicable, an IP subnet address. The ManageWise internetwork map displays segment icons and, for each segment, identifies the IPX network. If the network runs IP, the segment icon also has the address of the IP network (or subnet, if applicable) on that segment.

Network adapter

The hardware installed in workstations and servers that enables them to communicate on a network. *See also* **Adapter**.

Network address

The Network-layer address that refers to a logical network device. Also known as a *protocol address*.

Network management

The process of ensuring consistent reliability and availability of a network, as well as timely transmission and routing of data. Can be performed by dedicated devices or programmed general-purpose devices.

Network monitoring

The network management function that constantly checks the network and reports any problems.

Network segment

See **Segment**.

Network topology

The arrangement of nodes on a network—usually a star, ring, tree, or bus organization.

NLM

See **NetWare Loadable Module (NLM)**.

NLSP

See **NetWare Link Services Protocol (NLSP)**.

Node

A device that is connected to a network and is capable of communicating with other network devices. In NetWare, a node is considered to be an end system, such as a workstation.

ODI (Open Data-Link Interface)

The Novell specification that enables multiple LAN drivers and protocols to coexist on network systems. The ODI specification describes the set of interface and software modules used to decouple device drivers from protocol stacks and to enable multiple protocol stacks to share the network hardware and media transparently.

Packet

A unit of information transmitted as a whole from one device to another. In packet-switching networks, a transmission unit of fixed maximum size that consists of binary digits representing both data and a header.

Packet capture

The process of collecting packets using NetWare LANalyzer Agent for troubleshooting or problem isolation. You can specify a capture filter and display filter to collect or display only the packets or portions of packets you want. *See also* **Capture filter**, **Display filter**.

Packet decode

The process of displaying a captured packet so that you can see each protocol layer and field, and can also see the packet data in uninterpreted hexadecimal and either ASCII or EBCDIC format.

Packet display

The process of viewing packets online. ManageWise enables you to display a window showing a summary of all packets captured, a decoded packet (*see* **Packet decode**), and the packet data in hexadecimal and either ASCII or EBCDIC format.

Packet slice

A portion of a packet, counting from the packet header, measured in bytes. Because the header contains the most important data in a packet, you can specify a packet slice when capturing packets to economize on buffer space and minimize the load on NetWare LANalyzer Agent.

Physical address

The Data-Link layer address of a network device.

Pie chart

A circular graphic display of values, each occupying a wedge-shaped section of the pie. The size of the wedge represents its proportion to the other values (wedges) and to the whole.

Ping

A connectivity test in which an Internet Control Message Protocol (ICMP) echo request is sent. Connectivity is verified when a reply is received. *See also* **Connectivity test**.

Polling

Any procedure that sequentially and periodically contacts terminals in a network.

Port

As used in ManageWise, the connection to a repeater (other computer-related definitions exist). A port can be connected to a single adapter, to another repeater, or to another network segment (which can be a coaxial cable). *See also* **Repeater**.

Profile

A group of statistics that can be selected by name to display together in a graph, rather than displaying a single statistic. ManageWise enables you to select one profile by name and display a graph showing, for example, all errors or total utilization for a network segment. *See also* **SNMP profiles**.

Protocol

A set of rules that enables computers to connect with one another, specifying the format, timing, sequencing, and error checking for data transmission.

Protocol suite

A hierarchical set of related protocols.

Query

The process of extracting data from a database and presenting it for use.

RCONSOLE (Remote Console)

A NetWare utility that enables you to manage any NetWare 3 or later server on the internetwork remotely from one location.

Real-time data

The dynamic, current information ManageWise provides about a network, a segment, or a server. *Compare* **Trend data**, **Historic data**.

Remote monitor

An entity that collects information about the health of a network segment and stores the information so that it can be retrieved by management software. NetWare LANalyzer Agent is an example of a remote monitor.

Repeater

A device used to boost the strength of a signal; it is spaced at intervals throughout the length of a communications circuit. The repeater also handles collisions and other error conditions to provide correct operation of the network.

Router

A device that connects two networks using the same networking protocol. It operates at the Network layer (Layer 3) of the OSI model for forwarding decisions.

Routing protocol

A type of protocol that enables routing through the implementation of a specific routing algorithm. Examples of routing protocols include the Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, and Intermediate System-to-Intermediate System (IS-IS) protocol.

Routing table

A table stored in a router that keeps track of routes (and, in some cases, metrics associated with those routes) to a particular network destination.

Routing updates

A message sent from a router to indicate network reachability and associated cost information; it is typically sent at regular intervals and after a change in network topology.

Runt

A small Ethernet packet with FCS or alignment errors. Runts are the result of collisions occurring on a connected segment or between stations connected to attached repeaters. They are essentially "inferred collisions." Collisions between ports within the same repeater are detected explicitly. Runts are artifacts of collisions that cannot be detected explicitly because they are remote to the repeater observing the runt.

Segment

A component of a networking environment that corresponds to a physical cable. A segment is terminated by a bridge, a router, or any connecting device other than a repeater or hub. (ManageWise does not discover bridges, so sometimes ManageWise displays multiple bridged segments as a single segment.)

Segment consolidation

During the network discovery process, ManageWise might discover segments running both IP and IPX protocols and list them in the database as two segments. Segment consolidation combines the dual listings, making the database more accurate.

Segment map

A map of an Ethernet, token ring, or FDDI segment on a network showing the nodes that are attached to the segment.

Segment overconsolidation

On routers with NetWare MultiProtocol Router software and multiport WAN interfaces connected to different networks, ManageWise discovers the interfaces but not the ports. Therefore, all networks connected to an interface through its ports are interpreted as one network. *See also* **Segment consolidation**.

Server

A processor that provides a specific service to the network. Examples of servers are as follows:

—*Routing servers,* which connect nodes and networks of similar architectures

—*Gateway servers,* which connect nodes and networks of different architectures by performing protocol conversions

—*Terminal servers*, *printer servers*, *disk servers*, and *file servers*, which provide an interface between compatible peripheral devices on a   LAN

Short event

An Ethernet error that occurs when noise causes the repeater to initiate its normal packet repeat process. It is detected as short events by virtue of being shorter than the shortest possible collision fragment.

SNMP (Simple Network Management Protocol)

A protocol used to obtain management information about a network entity, such as a router or a network segment. In some cases, the information obtained from the device itself (for example, routers and hubs frequently have some management information that can be retrieved). In other cases, an agent collects information on behalf of the network entity (for example, a remote monitor collects information about segments it is attached to).

SNMP community name

A name used by SNMP for access control. The community name contained in an SNMP request must match the name expected by the device receiving the request. Different names can be used for different levels of access; for example, one name for retrieving information and another for setting values.

SNMP GET operation

A transaction request to read a specific value from a MIB table on a device.

SNMP GETNEXT operation

A transaction request to read the next value in a MIB table on a device.

SNMP POLL operation

A special request made to the SNMP Data Server to send a GET, GETNEXT, or SET transaction request periodically.

SNMP profiles

The files that record which SNMP variables should be retrieved by the SNMP MIB Browser and the type of visual display requested (table or graph).

SNMP SET operation

A transaction request to write a specific value to a MIB on a device.

Source address

The address of a sending network device.

Standard

A set of rules or procedures that have been agreed upon by industry participants.

Station

A node on a network, usually a workstation, but sometimes a server, hub, or router.

Table

A display of data in rows and columns. Generally, you can resize and rearrange the columns in a table, and you can sort the table based on the values in a selected column by double-clicking the column header.

TCP (Transmission Control Protocol)

The major transport protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams; it uses IP for delivery.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The protocol suite developed by the Advanced Research Projects Agency (ARPA); it includes TCP as the primary transport protocol and IP as the Network-layer protocol.

Threshold

See **Alarm threshold**.

Throughput

The total amount of useful information that is processed or communicated during a specific time period.

Ticker tape

A field on the ManageWise status bar that provides a horizontally scrolling display of alarm summary information. Alarms scroll across the ticker tape as they are received by the ManageWise Console.

Token

A special type of frame that is passed between token-passing LANs; possession of the token gives the possessor permission to transmit.

Token ring

A type of LAN that uses a circular (ring) topology and that accesses the media using a token (a special type of frame that, when held by a station, gives it permission to transmit).

Topology

The physical layout of network components (cables, stations, gateways, and hubs). Three basic interconnection topologies are star, ring, and bus networks.

Traffic data profile

See **Profile**.

Transaction

The computation to do a certain delimited amount of work, intended to be an indivisible action.

Trap

The unsolicited messages sent by an SNMP Agent to a network management system that indicate the occurrence of a significant event. The SNMP manager that receives a trap can poll for additional information. *See* **Alarm**.

Trend data

The information about the performance of network objects over time, for example, for the last hour or last 24 hours. *Compare* **Real-time data**.

Trend graph

A graph that displays trend data.

Unicast address

A type of address that specifies a single device.

Utilization

The percentage of a network resource being consumed by network events. *Network utilization* refers to the bandwidth being consumed by traffic. *Server CPU utilization* refers to the load on a given CPU. *Hub port utilization* refers to activity on a port.

Very long events

An Ethernet error that is presumed to be caused by continuously transmitting (jabbering) nodes. The repeater does not repeat the full length of such an event because it would cause faulty operation of certain network elements.

Virtual circuit

In packet-switching networks, a circuit that appears to be a physical point-to-point circuit. It connects two end points, conveying sequenced data packets reliably; in fact, it shares the underlying links and relay systems with other users of the network.

WAN

Wide area network. A network that transmits over large geographic areas using lines provided by a common carrier of private telecommunications facilities.

Workstation

The input/output equipment at which an operator works; the station in which a user can send data to, or receive from, a computer for the purpose of performing a job.

Index

F

G

H